Building Trust with Anchors

Eric Osterweil

Dan Massey

Lixia Zhang

What is DNSSEC and How it Works

- First, background on how DNSSEC actually works
- Just kidding…
  - Does anyone really want another DNSSEC 101?

What Do We Have Today

- Zone admins know their own DNSKEYs
  - Nominally, this info is held in a local file
- Some software is starting to bundle DNSKEY sets in local config files to bootstrap resolvers
  - Lets resolvers verify DNSSEC data out of the box
  - Useful in some ways, but…
  - What's the shelf-life of those keys?
  - Don't change that file, or when you update, you get your changes overwritten

Key Configuration Today

Software key file

+

Locally managed configuration

=

Using Local Files for Verification

- Thus, our starting point today is a set of two types of local files
- This structure has some clear benefits
  - Local verification can be done without introducing external (especially single) points of failure
  - Local knowledge can take precedence over 3rd party data
  - Ops can even remove keys that use "undesirable" crypto algorithms (i.e. GOST vs. RSA)

One More Step Completes the Spectrum

- What about keys that an operator believes should override or supplement the distro file, but not based on local knowledge?
  - Keys from web pages, newspapers, Ms. Cleo™, etc.
- One more type of file gives a sufficient set of basic trust management components
  - A ***TAR keys file***

Adding TARs to This

Vendor key file

+

Local config

+

Keys from TAR
(in the sky)

=

Managing Trust Anchors

- Will we always need local TAs?
  - I think yes (consider local knowledge if nothing else)
- Trust management should be done locally
  - Isolation from 3rd party failures
  - Local ground truth
  - Local policies
- Three basic elements facilitate this
  - Local configuration key file
    + TAR key file
    + vendor key file
- Now resolvers can function out of the box
- In addition, can still use local knowledge, preferences, and expertise to enhance operations

Thanks

Backup

DNSSEC Background

- DNSSEC provides *origin authenticity, data integrity,* and *secure denial of existence* by using public-key cryptography
- Origin authenticity:
  - Resolvers can verify that data has originated from authoritative sources.
- Data integrity
  - Can also verify that responses are not modified in-flight
- Secure denial of existence
  - When there is no data for a query, authoritative servers can provide a response that proves no data exists

How DNSSEC Works

- DNSSEC zones create public/private keys
  - Public portion goes in DNSSEC record type: DNSKEY
- Zones sign all RRsets and resolvers use DNSKEYs to verify them
  - Each RRset has a signature attached to it: RRSIG
- So, once a resolver has a zone's DNSKEY(s) it can verify that RRsets are intact by verifying their RRSIGs

Signing Example

Using a zone's key on a standard RRset (the NS)

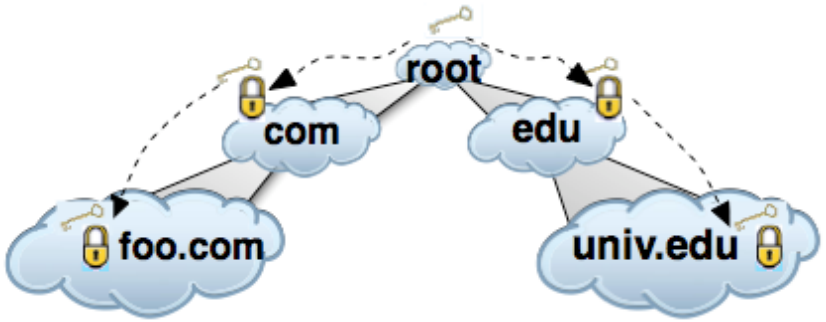
```
secspider.cs.ucla.edu.  3600    IN      NS      zinc.cs.ucla.edu.
secspider.cs.ucla.edu.  3600    IN      NS      alpha.netsec.colostate.edu.
```

Signature (RRSIG) will only verify with the DNSKEY if *no* data was modified

```
secspider.cs.ucla.edu.  3600 IN NS alpha.netsec.colostate.edu.
secspider.cs.ucla.edu.  3600 IN NS zinc.cs.ucla.edu.
secspider.cs.ucla.edu.  3600 IN RRSIG NS 5 4 3600 20080324024800 (
                                20080322024800 44736 secspider.cs.ucla.edu.
                                E4msde1nzVlfGvwDo2X6jLU5d9Xrk37lrYRCZN6yq5ad
                                mABa3B3KgKl13u2VBXDujJZucHSwPQMBy+JOmotZOggf
                                SgQWUYm86v8G7ABHHcI+YFD3z3eqSoAoBAE5ysafop1u
                                g7tw1J4xd/IADIVeu1HnVIKRSycILXzvCwcaDWwAd610
                                9oJUBSMgWZjGzYeJO9Rz0oUUqIqtn9PgVOzdTm+WnRC3
                                LEz50fdoP743QvPhe7RrF9w1KA3MOptTiQA++W8Gg085
                                NhbJ7MD99nEYaEv3+GuDCTkCy5ZOWoI/2Bcjq1NGBDLo
                                71lo6udu72i1tpyRfTEEQUirpInlZ9+IMw== )
```

Getting the Keys

- Until a resolver gets the DNSKEY(s) for a zone, data can be spoofed
- How can a resolver know that the DNSKEYs *themselves* are not being spoofed?



- DNSSEC zones securely delegate from parents to children
- Zones that have no secure parents are called trust anchors
- When a zone is a trust anchor the zones that it delegates to (and itself) form an *island of security*