DENIC DNSSEC Testbed
Software support for DNSSEC
Ralf Weber
(ralf.weber@nominum.com)
### Who is Nominum?

<table>
<thead>
<tr>
<th>Mission</th>
<th>Product Leadership</th>
<th>Industry Expertise</th>
</tr>
</thead>
</table>
| • Deliver the Trusted Internet Experience | • Best DNS Security  
• Highest Scalability  
• Highest Reliability  
• All Open Standards  
• Pioneered Intelligent DNS  
   Enabling rules and policies for every DNS request to protect end-users and ensure they reach their intended destination | • Dr. Paul Mockapetris  
Inventor of DNS, IETF Chair: 1994-1996  
Lifetime award: ACM SIGCOMM 2005 | • Bob Halley  
Co-Architect of BIND8  
Architect of BIND9 | • Ted Lemon  
Developer of ISC-DHCP  
Co-author of DHCP Handbook | • Over 30 Standards authored or co-authored |
| • Strategic Partners: | | |
| ![Yahoo](image)  
![Equinix](image)  
![Qwest](image)  
![Global Crossing](image)  
![BTE](image)  
![Verizon](image)  
![Colt](image)  
![Comcast](image)  
![Orange](image)  
![NTT Communications](image)  
![Telecom Italia](image)  
![Telefónica](image)  
![Deutsche Telekom](image)  
![Virgin Media](image) | |

**Securing the Worlds’ Largest Carriers DNS Infrastructure with Over 170M Broadband Households**
If verification is successful the DNS cache is populated with the A record, otherwise SERVFAIL is returned to clients.

* An appropriate NSEC record and RRSIG(NSEC) are sent if the domain does not exist or is not signed

** An appropriate NSEC record and RRSIG(NSEC) are sent if the domain does not exist
What can go wrong

- Every error in the chain of trust cause resolutions to fail
- Cryptography requires constant changes
  - Signatures and keys have limited lifetimes
  - DNS data becomes dynamic with static content
  - Cryptographic algorithm may change
- Software has to be kept up to date or may fail
- DNS Data becomes bigger
  - A lot of people still believe DNS packets have a maximum size of 512 Bytes and UDP only
  - DNS UDP packets with EDNS0 can get bigger and fragment
  - If that’s not enough DNS will switch to TCP
  - Not all network devices might understand this
DNS and network devices
DNSSEC network problems
DNSSEC and the network

● Clients are fine
  – They don’t do DNSSEC validation at the moment
  – Windows and MacOSX don’t have a validator
  – Only Fedora has and they screw it
  – The home gateway (9 out of 38) discussion only affects geeks
  – Home gateways have gotten better (Thanks AVM)

● Don’t run DNS servers behind firewalls
  – It is possible but it usually requires configuration
  – Firewalls are not made for high qps throughput (too much state)
  – They often break DNS servers defenses

● Load balancers should not alter DNS packets
  – Mostly applies for Global Server Load Balancing
  – You can use them for pure load distribution
Some DNSSEC statistics

- Number of DNSSEC domains (log scale)
Some DNSSEC statistics

- Number of Domains that fail validation
DNSSEC is gaining momentum
- It’s good to see some large registrar taking it in CZ.
- Some problems they might think about
  - All signatures expire at the same time
  - Do not resign or roll everything at once

Validation failures will be a problem
- We need to get operators the tools to mitigate them
- An insecure domain that resolves might be better than no resolving
- Who would customers call when amazon.com failed
Validation failures

● How do validation failures happen?
  – The data on the authoritative side is wrong
    • Signatures expired (arpa)
    • New keys without DS delegation at parent
    • Domain owner doesn’t care about DNSSEC any longer (register.bg ;-)

● What can we do that they not happen?
  – Don’t require 70 pages documents for people to setup DNSSEC
  – Make the operator interface the same as it used to be
    – Automate the resigning
    – Automate the key rollover
    – Automate the parent/child key relationship
Nominum products for DNSSEC

● All our software has been supporting DNSSEC for years
● We support NSEC, NSEC3 and all production algorithms
● Different software for caching and authoritative functions
● Vantio for DNS caching services
  – Fastest caching server with or without DNSSEC
● ANS for DNS authoritative services
  – In memory versioning database
● Configuration
  – All configuration is done on the running server and instantly active
  – No restart or file reload necessary
Seamless resolution of signed and unsigned zones

- Validation enabled for all domains under a defined trust anchor
- Add one line to configuration for ITAR
  - trust-anchor-file "/var/nom/vantio/anchors.mf";
- Possible to add more keys for islands of trust
  - trusted-keys { a0.com.invalid. 257 3 5 \ "AQO6CI+slAf +iuieDim9L3kujFHQD7s/IOj03ClMOpKYcTXtK4mRpuUL VfvWxDi9Ew/ gj0xLnnX7z9OJHIxLI+DSrAHd8Dm0XfBEAtVtJSn70GaPZ gnLMw1rk5ap2DsEoWk=" };  
- Possible to remove domains from validation if domain owners screw it
  - negative-trust-anchors { arpa.; register.bg.; };
Authoritative Server Challenges with DNSSEC

- Signing/resigning zones is CPU intensive
  - ANS leverages multi-core CPUs to sign most zones online, but out of ‘fast path’

- Database size can increase by 6x or more
  - ANS uses optimized database technology to handle large increases in data required by DNSSEC

- Key Administration

- Managing Signing of Zones

- Updating Zones When Data Changes
  - Manual zone file re-signing when records are added, changed or deleted from a zone (via DDNS or edits)

Solution is Nominum DNSSEC Packs
Nominum DNSSEC Packs

- An administrative bundle that manages DNSSEC lifecycle automation
  - Automatically sign/resign zones online
  - Automatically rollover keys (e.g. update after 60 days) based on policy
- All activities done via single command utility (“ans_dnssectool”)

![Diagram of DNSSEC Pack system]

- (Optionally) Encrypted
- DNSSEC Pack Database
  - (Optionally) Store on removable media (e.g. USB drive)
  - Manage lifecycle based on configuration
Securing a zone

To secure a previously insecure zone, create a pack for it.
- `ans_dnssectool create-pack --name initial example.com`

What this does:
- Creates a KSK for the zone. The default is a 2048-bit RSA/SHA1 key.
- Creates a ZSK for the zone. The default is a 1024-bit RSA/SHA1 key.
- Gives the initial signing-data the name "initial" (used in logging)

Result:
- The server will immediately begin signing the zone
- Publishes it when signing completes
- Server logs the publishing progress
- Automatically resigns zone before signatures expire
- New records are automatically signed with current keys

Online signing support is key to allowing tools to handle signing as transparently as possible
What we mean by transparency
The hostmasters view

Insecure zone
@ 300 IN SOA (ns1 hostmaster
   1265702400
   3600
   600
   2592000
   300 )
@ 300 IN NS ns1
@ 300 IN NS ns2
ns1 300 IN A 192.0.2.1
ns2 300 IN A 192.0.2.2
www 300 IN A 192.0.2.3

Secure zone
@ 300 IN SOA (ns1 hostmaster
   1265702400
   3600
   600
   2592000
   300 )
@ 300 IN NS ns1
@ 300 IN NS ns2
ns1 300 IN A 192.0.2.1
ns2 300 IN A 192.0.2.2
www 300 IN A 192.0.2.3
And that is what other software or the wire give you
Example: ZSK rollover

- Periodically you will want to update your ZSK
  - All that is required as input is the time to do the update

- `ans_dnssectool rollover-zsk --name autumn-zsk --start 20100715211800 example.com`

- Signatures using the new ZSK will be published at 21:18 UTC on July 15, 2010.
  - New keys will be generated and start being used automatically

- You can provision multiple ZSK key rollovers that all will be stored in the database and executed appropriately
3 Levels of Security

- Default Security
- Increased Security
- High Security
Default Security

- Private KSK not in readable format on disk
  - Optionally stored on removable disk (e.g. USB drive)
Increased Security

- DNS queries to ANS
- ZSK is stored here
- Online updates of secure zones
- KSK is stored here
- DNSSEC configuration done here
- Secure Server (DNSSEC pack created here)

Manual transfer of DNSSEC pack:
- DNSSEC pack data transferred by file
- Transfer over network or manually (e.g. USB drive)

Online updates of secure zones
High Security

- No private keys stored here
- No DNSSEC configuration done here
- (zsk & ksk) All private keys
- All zone signing done here

**DNS queries**

**ANS**

- No online updates of secure zones
- Manual transfer of signed zone data
  - if ANS and secure server are network connected, do zone transfer
  - else, dump contents and manually (e.g. USB drive) load on ANS

**Secure Server (running copy of ANS)**
A word on NSEC3

- NSEC3 is not better than NSEC
- It solves two problems most people don’t have
  - Data privacy for zones
  - Large delegation centric zones with only few secure delegations
- Data privacy is given by obfuscating the pointer to the next record
  - The next entry is not the name but a hash of the name
  - To make it even worse the hash can be called more than once
  - Computation of hash functions use CPU time
- Opt out NSEC3 records make validation a bit more complicated
  - They tell what parts of the zone are not secured
  - Validator has to check this
Questions?