DNSSEC Deployment
a case study

Olaf M. Kolkman
Olaf@NLnetLabs.nl

RIPE NCCs Project Team:
Katie Petrusha, Brett Carr, Cagri Coltekin, Adrian Bedford, Arno Meulenkamp, and Henk Uijterwaal
Presentation roadmap

• Overview of problem space
  – DNSSEC introduction
  – Architectural changes to allow for DNSSEC deployment

• Deployment tasks
  – Key maintenance
  – DNS infrastructure
  – Providing secure delegations
Why DNSSEC

• Good security is multi-leveled
  – Multiple defense rings in physical secured systems
Why DNSSEC

• Good security is multi-leveled
  – Multiple defense rings in physical secured systems
  – Multiple ‘layers’ in the networking world

• DNS infrastructure
  – Providing DNSSEC to raise the barrier for DNS based attacks
  – Provides a security ‘ring’ around many systems and applications
DNSSEC evangineer of the day

- **NLnet Labs** ([www.NLnetLabs.nl](http://www.NLnetLabs.nl))
  - Not for profit Open Source Software lab
    - NSD, open source nameserver
  - DNS and DNSSEC research
    - Protocol and software development
    - Deployment engineering
- **Co-Chair of the IETF DNSEXT working group**
The Problem

- DNS data published by the registry is being replaced on its path between the “server” and the “client”.
- This can happen in multiple places in the DNS architecture
  - Some places are more vulnerable to attacks than others
  - Vulnerabilities in DNS software make attacks easier (and there will always be software vulnerabilities)
DNS Architecture

Provisioning

DN Protocol

http://www.nlnetlabs.nl/
DNS Architecture

Server compromise

Inter-server communication

Cache Poisoning

Provisioning

DNS Protocol

Registry DB

Registrars

http://www.nlnetlabs.nl/
Example: Unauthorized mail scanning

Big Corp Mail Server -> Important Corp Mail Server

Where? There!

DNS
Example: Unauthorized mail scanning

Big Corp Mail Server

Where?

Elsewhere

DNS

Bad Guy

Important Corp Mail Server
Targets…
Where do DNS and economics meet?

• SPF, DomainKey and family
  – Technologies that use the DNS to mitigate spam and phishing: $$$ value for the black hats

• Stock tickers, RSS feeds
  – Usually no source authentication but supplying false stock information via a stock ticker and via a news feed can have $$$ value

• ENUM
  – Mapping telephone numbers to services in the DNS
DNSSEC properties

- DNSSEC provides message authentication and integrity verification through cryptographic signatures
  - Authentic DNS source
  - No modifications between signing and validation
- It does not provide authorization
- It does not provide confidentiality
Metaphor

• Compare DNSSEC to a sealed transparent envelope.
• The seal is applied by whoever closes the envelope
• Anybody can read the message
• The seal is applied to the envelope, not to the message
RIPE Regional Meeting, Qatar, Januari 2006

http://www.nlnetlabs.nl/

nlnetlabs.nl. 86400 IN NS omval.tednet.nl.
nlnetlabs.nl. 86400 IN RRSIG NS 5 2 86400 20060131005003 (20060101005003 43791 nlnetlabs.nl.
y9URn71LgxDPh2MY/I/CRkmG5PZ2nJQxndGHwSB8OP15 [...]Qg1+bOoj54b/65TyYVqPp3CLVt/q6L67SMK9orE= )
nlnetlabs.nl. 86400 IN DNSKEY 257 3 5 (AQPzzTWMz8qSWIQLfRnPckx2BiVmkVN6LPupO3mbz7Fh [...]9QP7y2bVw5zSbFCrefk8qCUBgfHm9bHzMG1UBYtEIQ== ); key id = 43791
nlnetlabs.nl. 86400 IN RRSIG DNSKEY 5 2 86400 20060131005003 (20060101005003 43791 nlnetlabs.nl.
6mEWVaFKLQrypCJb0w gzW56UC1SVGYW3z+KJVM/uANnA [...]4cCBqAX/mE2N5nUZians0/IT1TzuqVS5h12R2jE= )
onopen.nlnetlabs.nl. 86400 IN RRSIG A 5 3 86400 20060131005003 (20060101005003 43791 nlnetlabs.nl.
ZoZl6om+q5e4jrrDB64mMXpiloCQVe6NDu7KZbv7k9fg [...]t+Xc4iQPI+HTPn5A18pjaEA9KAK7NFLTZHz5uV8= )
onopen.nlnetlabs.nl. 86400 IN RRSIG AAAA 5 3 86400 20060131005003 (20060101005003 43791 nlnetlabs.nl.[...]
Presentation roadmap

• Overview of problem space
  – DNSSEC introduction
  – Architectural changes to allow for DNSSEC deployment

• Deployment tasks
  – Key maintenance
  – DNS infrastructure
  – Providing secure delegations
DNSSEC

Architecture modifications

- Zone Creation
- Provisioning DB
- DNS and input checks
- Zone signer
- Primary DNS
- Secondary DNS
- DNSSEC aware servers
- Customer interfaces
- DNSSEC aware provisioning

http://www.nlnetlabs.nl/
DNSSEC deployment tasks

• Key maintenance policies and tools
  – Private Key use and protection
  – Public key distribution

• Zone signing and integration into the provisioning chain

• DNS server infrastructure

• Secure delegation registry changes
  – Interfacing with customers
Overview of problem space
  - DNSSEC introduction
  - Architectural changes to allow for DNSSEC deployment

Deployment tasks
  - Key maintenance
  - DNS server infrastructure
  - Providing secure delegations
Key Maintenance

- DNSSEC is based on public key cryptography
  - Data is signed using a private key
  - It is validated using a public key

Operational problems:

- Dissemination of the public key
- Private key has a ‘best before’ date
  - Keys change, and the change has to disseminate

http://www.nlnetlabs.nl/
Public Key Dissemination

• In theory only one trust-anchor needed that of the root
  – How does the root key get to the end user?
  – How is it rolled?

• In absence of hierarchy there will be many trust-anchors
  – How do these get to the end-users?
  – How are these rolled?

• These are open questions, making early deployment difficult.
Public Key Dissemination at RIPE NCC

In absence of a signed parent zone and automatic rollover:

• Trust anchors are published on an “HTTPS” secured website
• Trust anchors are signed with the RIPE NCC public keys
• Trust anchor will be rolled twice a year (during early deployment)
• Announcements and publications are always signed by x.509 or PGP
Key Management

• There are many keys to maintain
  – Keys are used on a per zone basis
    • Key Signing Keys and Zone Signing Keys
  – During key rollovers there are multiple keys
    • In order to maintain consistency with cached DNS data [draft-ietf-dnsop-dnssec-operational-practices]

• Private keys need shielding
Private Key Maintenance

Basic Architecture

- Zone DB
- Signer client
- DNS server
- Key maintainer
- Key DB and Signer server
- KEY Master

http://www.nlnetlabs.nl/

RIPE Regional Meeting, Qatar, January 2006
Maintaining Keys and Signing Zones

• The KeyDB maintains the private keys
  – It ‘knows’ rollover scenarios
  – UI that can create, delete, roll keys without access to the key material
  – Physically secured

• The signer ties the Key DB to a zone
  – Inserts the appropriate DNSKEYs
  – Signs the zone with appropriate keys

• Strong authentication
Private Key Maintenance
The software

- Perl front-end to the Bind dnssec-signzone and
dnssec-keygen tools
- Key pairs are kept on disc in the “Bind format”
- Attribute files containing human readable information
  - One can always bail out and sign by hand.

- Works in the RIPE NCC environment, is a little rough edged but available via the
  www.ripe.net/dis
Example session

$ maintkeydb create KSK RSASHA1 2048 example.net
Created 1 key for example.net

$ maintkeydb create ZSK RSASHA1 1024 example.net
Created 2 keys for example.net

$ dnssigner example.net
Output written to :example.net.signed

$ maintkeydb rollover zsk-stage1 RSASHA1 example.net
Presentation roadmap

- Overview of problem space
  - DNSSEC introduction
  - Architectural changes to allow DNSSEC deployment

- Deployment tasks
  - Key maintenance
  - DNS server infrastructure
  - Providing secure delegations
Infrastructure

- One needs primary and secondary servers to be DNSSEC protocol aware

- We had a number of concerns about memory CPU and network load
  - Research done and published as RIPE 352
  - What follows are the highlights of that paper
Question

What would be the immediate and initial effect on memory, CPU and bandwidth resources if we were to deploy DNSSEC on RIPE NCC’s ‘primary’ name server?

- Measure through simulation.
- Published in RIPE352
Memory

- On ns-pri.ripe.net factor 4 increase.
  - From ca. 30MB to 150MB
  - No problem for a 1GB of memory machine
- On k.root-servers.net
  - Increase by ca 150KB
  - Total footprint 4.4 MB
- Nothing to worry about
- Memory consumption on authoritative servers can be calculated in advance.
  - No surprises necessary
Serving the zones Query Properties

- DNS clients set the “DO” flag and request for DNSSEC data.
  - Not to do their own validation but to cache the DNSSEC data for.
- EDNS size determines maximum packet size.
  (DNSSEC requires EDNS)
- EDNS/DO properties determine which fraction of the replies contain DNSSEC information
EDNS properties

- k.root DNS Packets
- k.root EDNS size Distribution
- EDNS size for "DO" queries in k.root

- ns-pri DNS Packets
- ns-pri EDNS Size Distribution
- EDNS size for "DO" queries in ns-pri

http://www.nlnetlabs.nl/
<table>
<thead>
<tr>
<th>trace</th>
<th>server</th>
<th>ZSK size</th>
<th>WCPU</th>
</tr>
</thead>
<tbody>
<tr>
<td>ns-pri</td>
<td>BIND 9.3.1</td>
<td>0000</td>
<td>ca 14%</td>
</tr>
<tr>
<td>ns-pri</td>
<td>BIND 9.3.1</td>
<td>2048</td>
<td>ca 18%</td>
</tr>
<tr>
<td>k.root</td>
<td>BIND 9.3.1</td>
<td>0000</td>
<td>ca 38%</td>
</tr>
<tr>
<td>k.root</td>
<td>BIND 9.3.1</td>
<td>2048</td>
<td>ca 42%</td>
</tr>
<tr>
<td>k.root</td>
<td>BIND 9.3.1</td>
<td>mod 2048</td>
<td>ca 50%</td>
</tr>
<tr>
<td>k.root</td>
<td>NSD 2.3.0</td>
<td>0000</td>
<td>ca 4%</td>
</tr>
<tr>
<td>k.root</td>
<td>NSD 2.3.0</td>
<td>2048</td>
<td>ca 4%</td>
</tr>
<tr>
<td>k.root</td>
<td>NSD 2.3.0</td>
<td>mod 2048</td>
<td>ca 5%</td>
</tr>
</tbody>
</table>
Bandwidth Factors

- fraction of queries with DO bit
  - Seen in difference between ns-pri and k.root result
  - Seen in difference between modified and unmodified servers
- Including DNSKEY RR in additional section.
  - Seen in difference between k.root traces from modified nsd and modified named
- Difference in answer patterns
  - Name Errors vs Positive answers
  - Difficult to assess from this data

http://www.nlnetlabs.nl/
Bandwidth increase when all queries to k.root-servers.net would request for DNSSEC

With DNSSEC

Without DNSSEC
Bandwidth Increase

• Significant for ns-pri.ripe.net
  – Well within provisioned specs.
• Insignificant for k.root-servers.net
  – Upper bound well within provisioning specs

(Key size influences bandwidth but bandwidth should not influence your key size)
Conclusion of these measurements

- CPU, Memory and Bandwidth usage increase are not prohibitive for deployment of DNSSEC on k.root-servers.net and ns-pri.ripe.net

- Bandwidth increase is caused by many factors
  - Hard to predict but fraction of DO bits in the queries is an important factor

- CPU impact is small, Memory impact can be calculated

- Don’t add DNSKEY RR set in additional
Presentation roadmap

• Overview of problem space
  – DNSSEC introduction
  – Architectural changes to deployment

• Deployment tasks
  – Key maintenance
  – DNS server infrastructure
  – Providing secure delegations
Parent-Child Key Exchange

• In the DNS the parent signs the “Delegations Signer” RR
  – A pointer to the next key in the chain of trust

• DNSKEY or DS RR needs to be exchanged between parent and child
Underlying Ideas

• The DS exchange is the same process as the NS exchange
  – Same authentication/authorization model
  – Same vulnerabilities
  – More sensitive to mistakes

• Integrate the key exchange into existing interfaces
  – Customers are used to those

• Include checks on configuration errors
  – DNSSEC is picky

• Provide tools
  – To prevent errors and guide customers
How Did we Proceed

• The ds-rdata: attribute was added to the Domain object
• The zone generation tool: extract DS RR from ds-rdata: attributes
• We introduced a filter, to block ds-rdata: for zones not yet signed
• Added a number of “DelChecker” checks
Intergration issue

• Thinking about DNSSEC made the NCC look at the provisioning system as a whole
  – Prompted a couple of modifications
  – Zone generation (generation of zone now from the Whois DB)
  – Authentication model (introduction of mnt-domain)
  – Possible replay attacks (countered by using timestamps of the strong auth. mechanisms)
• All these issues are NOT DNSSEC specific
• Addressed over the last 2 years
Introducing the Web Interface

• Eases registration of keys and the rollovers
  – Can also be used for “classic” delegations

• Restrictions user somewhat
  – Fewer degrees of freedom mean fewer errors
  – One can always manually create the Domain object

• Version 1 to appear shortly
  – Demo in the hallway
Web Interface Examples

May the Demo Gods be with us.

We’ll cheat.
NCC Roadmap

• RIPE NCC is signing its zones
  – Forward zones (ripe.net &c) are signed
  – Signatures are still being introduced in reverse zones (v4 and v6)
• Secure Delegations available for a number of /8 equivalent zones
• Policy and procedures available
  – www.ripe.net/reverse
QUESTIONS?

Acknowledgements: A number of these slides are based on earlier work at RIPE NCC.

http://www.nlnetlabs.nl/   RIPE Regional Meeting, Qatar, Januari 2006