Commencing countdown: DNSSEC on!
USENIX LISA ’10, San Jose, CA

Roland van Rijswijk
roland.vanrijswijk [at] surfnet.nl

November 10th, 2010
About SURFnet

National Research and Education Network (NREN)

Founded in 1986

10628 km (±6604 mi.) of fibre-optic cables for an ultra high-bandwidth network

‘Shared ICT innovation centre’

≥ 160 connected institutions
±1 million end-users
Overview

- Intro & short recap: DNSSEC, why & what?
- Resolving
- Operating signed zones
- Lessons learned
- Monitoring
- Conclusion & questions
Why attack DNS?

- DNS is **everywhere**:
  - In your phone, in your laptop, in your PC...
  - But also in your car, in an ATM, in your elevator, ...

- It is very hard to protect plain DNS against attacks

- It is very easy to attack a lot of users
DNS attack vectors

- Queries
- Dynamic updates
- Zone transfers
- Man in the middle
- Cache poisoning
- Data modification
- Data modification
- Spoofed updates
- Corrupt data

Stub resolver

Caching resolver

Primary

Secondaries

Zone file
Cache poisoning
Bad news...

http://lambicpeach.files.wordpress.com/2008/10/badnewspup.jpg

SURFnet. We make innovation work
Good news :-)
What is DNSSEC?

- DNSSEC was first devised in 1997

- We are at the third generation of the protocol
  - DNSSEC (ca. 2000)
  - DNSSECbis (2005)
  - NSEC3 (2008)

- Some 20 (!) active RFCs
  - That’s excluding the ‘normal’ DNS RFCs

- Protocol is mature
  - Changes are mainly new algorithms
What is DNSSEC?

- Digital Signatures guarantee authenticity of DNS records
  - Like a wax seal

- Resolvers validate the signatures and discard records with bogus signatures

- DNSSEC only provides authenticity
  - So no confidentiality
  - nor protection against DDoS
  - or typosquatting, phishing, etc.
Deployment status

- Root was signed on July 15th

- Signed generic TLDs: .asia, .biz, .cat, .edu, .gov, .info, .museum, .org, .net (end of 2010), .com (March 2011)

- Signed ccTLDs: 37 countries & counting

- Registrars are starting to support DNSSEC (28 .org registrars -- source: PIR)
- The validation rates has risen significantly since the root got signed:
Operating a validating resolver
Software

- The majority of DNS resolvers support DNSSEC out-of-the-box:

<table>
<thead>
<tr>
<th>Product</th>
<th>DNSSEC</th>
<th>RFC 5011</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISC BIND</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Unbound</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>djbdns</td>
<td>No</td>
<td>n/a</td>
</tr>
<tr>
<td>MaraDNS</td>
<td>No</td>
<td>n/a</td>
</tr>
<tr>
<td>Microsoft DNS</td>
<td>Yes</td>
<td>No*</td>
</tr>
<tr>
<td>Simple DNS Plus</td>
<td>Yes</td>
<td>No**</td>
</tr>
<tr>
<td>Nominum Vantio</td>
<td>Yes</td>
<td>No**</td>
</tr>
</tbody>
</table>

* Confirmed
** Not specified in product documentation
Trust anchor configuration

- You should seriously consider using a resolver that supports RFC 5011
- Check the validity of your trust anchor(s) at regular intervals
- **Validate** a trust anchor before using it!

\[\text{IN DS 19036 8 2} \quad 49A{\text{AC11D7}}6{\text{F6446702E54A160737160}}
7{\text{A1A41855200FD2CE1CDDE32F24E8FB5}}
xidep-pybec-tyvak-zonag-kesud-vohip-cumul-fysuk-bivac-pubam-
hugeb-buzud-symes-tylaf-dosog-vufor-huxax\]
Setting up a validating resolver

- HOWTO instructions for BIND: https://dnssec.surfnet.nl/?p=402

- HOWTO instructions for Unbound: https://dnssec.surfnet.nl/?p=212

- Shameless advert: use (or try) Unbound!

http://unbound.net
Checking your setup (1)

- Perform a lookup of a record known to be signed, for instance: www.iis.se:

$ dig +dnssec +noauth www.iis.se @myresolver
...
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 51109
;; flags: qr rd ra ad
QUERY: 1, ANSWER: 2,...

;; ANSWER SECTION:
www.iis.se. 50 IN A 212.247.7.221
www.iis.se. 50 IN RRSIG A 5 3 60 20101111213001
20101101213001 23384 iis.se.
BiKEZgxBf4KASooHPwYJ7Dld/

...
Checking your setup (2)

- Visit one of the DNSSEC test sites such as:
  http://www.nic.cz/dnssec
  http://www.dnssec-failed.org
  http://test.dnssec-or-not.org/ <-- funny

- And verify the result:

source: nic.cz
Dealing with validation failures

- Validation failures will lead to the resolver returning **SERVFAIL**

- Clients will try **all configured resolvers**
  - If one of them doesn’t validate, the query will succeed and the user probably only notices a slight delay

- In our experience, users don’t call the helpdesk
  - So no: “The Internet is broken”

- Nevertheless: if you see validation failures then try to alert the zone owner

Impact on resource use

- DNSSEC relies on public key cryptography
  - Crypto eats CPU cycles, right?

- We’ve been running with full validation enabled since the start of last year

- The impact on CPU load is negligible
  - Measuring doesn’t show a significant difference
  - Remember: DNS resolving is all about **caching results**
Validation rate

- Remember that odd spike in the validation rate?
I asked blogreaders:
Puzzle solved

Hugo Salgado (@huguei) showing my ASCII art pie

SURFnet. We make innovation work
Troubleshooting

- DNSSEC relies on the EDNS0 extension (RFC 2671)
  - For larger messages (signatures)
  - For the DO-bit (DNSSEC OK)

- Some network hardware has problems with DNSSEC traffic

- Firewalls are notorious for blocking:
  - UDP packets over 512 bytes in size
  - Fragmented UDP packets
  - TCP on port 53

- CPE/SOHO routers also cause trouble
Operating a signed zone
Why sign your zone?

- Because your website represents a valuable asset for your organisation

- To prevent redirection of Internet traffic to your domain (think: VoIP, e-mail, etc.)

- To protect your users

- To leverage the trust that DNSSEC can establish
  - DNSSEC is a PKI
  - store SSH fingerprints in DNS (SSHFP record)
  - store X.509 certificates in DNS (CERT record)

- Because your competitor does it too :-)

28
User study

- We did a user study among our constituency
  - 169 persons asked to participate
  - 38 responded representing 37 organisations (academia, research institutions, teaching hospitals)

- Two-thirds of users feel DNSSEC is important:

- > 75% plan to sign their domain:
When to sign your zone?

- Your infrastructure should be ready
  - Remember the firewall trouble mentioned when resolving was discussed

- You should have a clear mandate
  - DNS affects everything on your network so DNSSEC does too

- Think before you act :-) 

- The way back is harder than the way forward
How to sign your zone: case study SURFnet

- SURFnet operates a managed DNS environment called ‘SURFdomeinen’

- We ran a project this year from Q1 to Q3 to implement DNSSEC in SURFdomeinen

- Our goals:
  - To make it easy for our connected institutions to operate signed zones
  - To make it easy for ourselves to operate signed zones

- We enabled DNSSEC for surfnet.nl at the end of September

donderdag 11 november 2010
Requirements

- DNSSEC should be a ‘box to tick’
  - DNS is already considered to be complex by many users, something that doesn’t improve if you add DNSSEC

- The integrity of zones should be guaranteed
  - SURFdomedinen should not be the ‘weakest link’ in the attack chain
  - Monitoring is of great importance (more on that later)

- Turning DNSSEC on or off should not take too long
  - Ideally less than 1 hour

- Once DNSSEC is turned on, customers should not notice any difference
Design decision: using HSMs

- HSM = Hardware Security Module
- Secure and robust way to store DNSSEC key material
- We can never access the raw key material
- Role separation
- Standard API (PKCS #11)
- Disadvantage: expensive
Design decision: OpenDNSSEC

- SURFnet participates in the project
  - Other partners are: IIS (.se), Nominet (.uk), Kirei, SIDN (.nl), NLnet Labs en Sinodun

- Goal: push-the-button signing

- Functions like a ‘bump-in-the-wire’

- Possibility to have different policies for different customers

- Possibility to share keys (e.g. one set of keys per customer rather than per zone)
Design decision: OpenDNSSEC

- OpenDNSSEC 1.1
  - Current version; used in production by a number of top-level domains and also for our deployment
  - Used - for instance - by .uk, .fr, .se and .nl

- OpenDNSSEC 1.2 (end of Q4 2010)
  - First beta version has been released
  - Faster signer engine in C
  - Better support for ‘key-sharing’

- OpenDNSSEC 1.3 (±Q2 2011)
  - Design is underway
  - Performance improvements for larger setups (50000+ zones)
  - Multi-threaded signer for better performance
  - SURFnet and IIS (.se) investing in extra development effort
OpenDNSSEC architecture
Design: bump-in-the-wire

DNS zone

Internet

Hidden primary → DNS transfer → Public primary

OpenDNSSEC

Internet

Hidden primary → DNS transfer → OpenDNSSEC → DNS transfer → Public primary
Design: data flow
Design: network security
Design: redundancy

Signer:

- Warm standby system in a different co-location
- MySQL master-slave replication
- Failover is a manual process (not time critical)

HSM:

- Two HSMs in two different locations
- High-availability mode
- Offline secure backup on a third location
- Keys will only be used after a backup
Enabling DNSSEC: user perspective

- Push-the-button signing:

DNSSEC
DNSSEC is uitgeschakeld voor deze zone
DNSSEC is een DNS extensie die de afkomst van DNS gegevens authenticeert. Daarmee is de zone beter beschermd tegen bedreigingen zoals DNS Cache Poisoning.

DNSSEC inschakelen

DNSSEC
Aanvraag voor inschakeling loopt
De aanvraag om DNSSEC in te schakelen wordt behandeld door SURFnet. U ontvangt een e-mail wanneer DNSSEC voor deze zone is ingeschakeld.

DNSSEC uitschakelen

- Unsigned to signed in 15 minutes

DNSSEC
DNSSEC is ingeschakeld voor deze zone
Wilt u deze zone verhuizen? Geef de andere DNS operator de publieke DNS-key van deze zone. Bekijk het DNSKEY-record voor deze zone

DNSSEC uitschakelen
Monitoring

- Monitoring helps to detect problems early-on

- When monitoring a signed zone, look for:
  - Signature expiry
  - MTU problems (firewalls!)
  - Continuous validation

- Also monitor from outside your own network

- Many tools are available, for example:
  [http://www.dnssecmonitor.org](http://www.dnssecmonitor.org)
  [http://www.dnsviz.net](http://www.dnsviz.net)
Advice for getting started

- Make use of available tooling
  - OSS: OpenDNSSEC, BIND
  - Commercial signer solutions

- Make sure you have good monitoring

- Write down policies and procedures

- Carefully think about your design

- Make your users’ life easy!

- Check with your secondaries for DNSSEC support
Signer software (1)

- Of course there’s not just OpenDNSSEC; there are lots of open source solutions:

- **BIND 9.x**
  - Key storage in the clear on disk
  - HSM support only through *patched* OpenSSL
  - No automated key rollover (scriptable though)

- **BIND 10**
  - Still heavily under development (5 year project)
  - Alpha versions have been released

- **PowerDNSSEC**
  - Alpha release available

- **ZKT (Zone Key Tool)**
  - No longer seems to be maintained
Signer software (2)

- Secure64 DNS signer
  http://www.secure64.com

- Xelerance DNS-X signer
  http://www.xelerance.com

- IPAM vendors
  - Men & Mice
  - Infoblox
  - BlueCat networks
  - ...

- Microsoft Windows Server 2008R2
When things go wrong...

LAST TRANSACTION CANCELLED

PLEASE TAKE YOUR CARD

Windows - Virtual Memory Minimum Too Low

Your system is low on virtual memory. Windows is increasing the size of your virtual memory paging file. During this process, memory requests for some applications may be denied. For more information, see Help.

Photo courtesy of jeffwilcox@FlickR
Admitting mistakes

Sorry NO
INTERNET Today
AXFR bug in OpenDNSSEC

- surfnet.nl was signed for the first time in September (on a Monday)

- everything went smoothly until Thursday

- then suddenly...
  - no more mail
  - no more website
  - no more VoIP

- D’oh!!!

- Garbage In --> Garbage Out

- AXFR bug in OpenDNSSEC has been fixed

donderdag 11 november 2010
Stories from the trenches...

- .cz and .us became ‘bogus’ because of a mistake during an algorithm rollover

- ISOC & .org nearly had a PR disaster at ICANN 38 in Brussels

- .uk became ‘bogus’ because of a glitch during a signer failover

- .be forgot to update critical signatures

- mozilla.org and nasa.gov published a DS while there zone wasn’t signed yet
If you’re lucky...

- this is what users will see:

many thanks to Marco Davids of SIDN for the screenshot
But in most cases...

- this is what users will see:

- (and this is better IMHO!)
Contacting domain owners is hard
So what have we learned?
2,724 visits came from 81 countries/territories
Other resources

- [http://dnssec.net](http://dnssec.net)
  - Comprehensive and up-to-date links to information on DNSSEC

- [SURFnet white-paper](http://www.dnssec.nu)
  - In fairness: not 100% up-to-date but useful nevertheless

- [http://www.dnssec-deployment.org](http://www.dnssec-deployment.org)
  - Tracks DNSSEC deployment across the net

- [http://www.practicesafedns.org](http://www.practicesafedns.org)
  - PIR (.org) initiative with user stories
Conclusions

- DNSSEC deployment has taken off
- The ball is now in your court!
- Seriously consider enabling validation on your resolver
- Think about signing
- Don’t be afraid to admit mistakes
  - A lot can be learned from them!
- Once it works, you don’t notice it’s there
That’s all folks! Questions?

Thank you for your attention!

Roland van Rijswijk
roland.vanrijskij [at] surfnet.nl
@reseauxsansfil

Presentation release under the Creative Commons “Attribution” license:
(http://creativecommons.org/licenses/by/3.0/)

Disclaimer: all cartoons and photos in this presentation were taken from the Internet. Though care has been taken to trace the owner and the license and to add attribution where necessary, if you feel your copyright has been infringed please contact me.