A bird's-eye view on DNSSEC

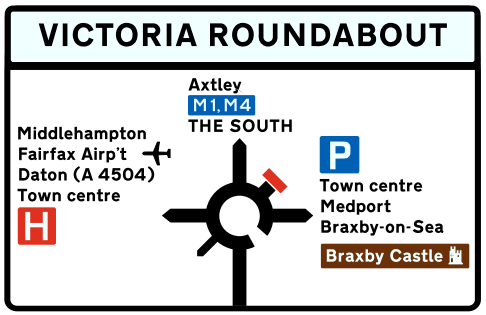
UKUUG Spring 2011 Conference
Leeds, UK
March 2011

Jan-Piet Mens

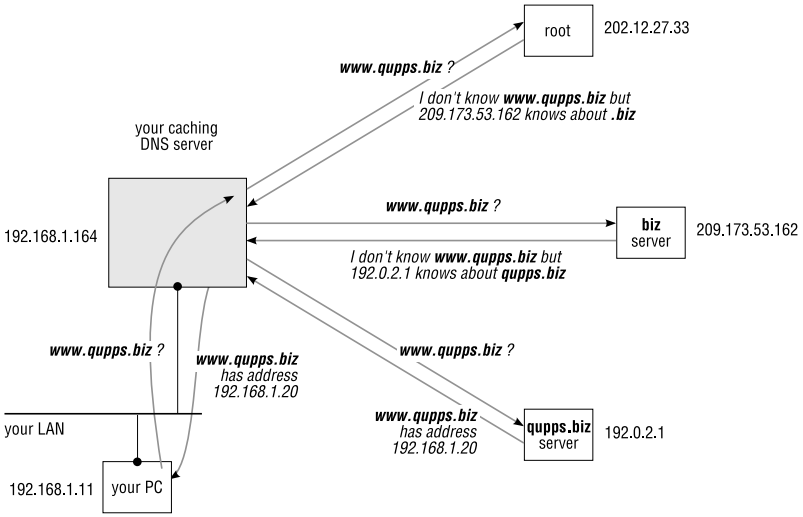
```
$ dig 1.1.0.3.3.0.8.1.7.1.9.4.e164.arpa naptr
```

DNS is easy

- Ask a question, get a reply.
- Ask a question, get a referral:
  - Susie: what's Caroline's number? Ask Thomas.
  - Thomas: Caroline's number? Ask Diana.
  - Diana: Caroline's number: 0123456789

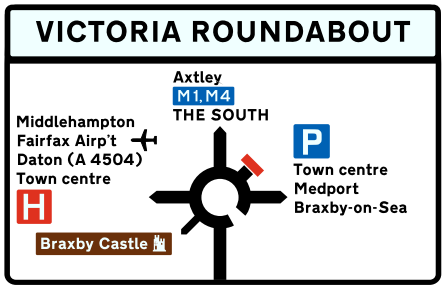


Resolution



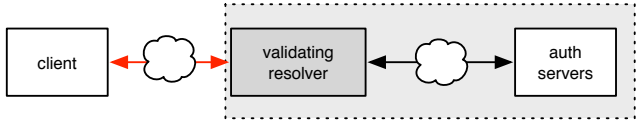
The problem

- DNS is insecure: one packet for query, one packet for response; easily spoofed
- Is this really Amazon?
  - https://amazon.de
- DNS Spoofing & cache poisoning
  - DNS server accepts and uses data from a host which shouldn't have been allowed to provide reply



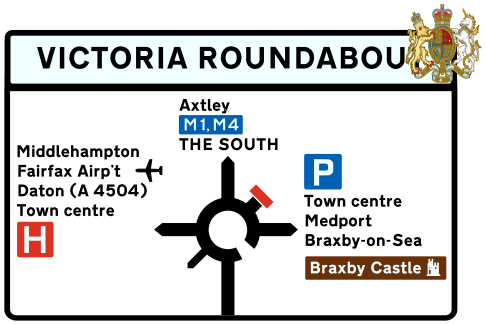
The solution

- DNSSEC
  - Eliminates known cache-poisoning attacks & cache-manipulation
  - Public key cryptography and digital signatures
    - provide data origin authentication
    - provide data integrity
  - Doesn't encrypt data -- that would be stupid
  - But: not end-to-end. (From validating cache to auth. server only.)
    - Install validating cache "close" to you



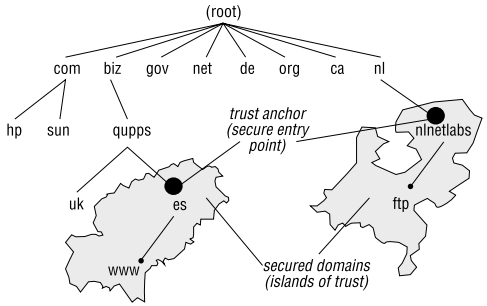
DNSSEC is (rather) easy

- Ask question, get reply and signature
- Ask question, get referral and signature
  - Susie: Caroline's number? Ask Thomas.
  - Thomas: Caroline's number? Ask Diana.
  - Diana: Caroline's number: 0123456789



How does DNSSEC work?

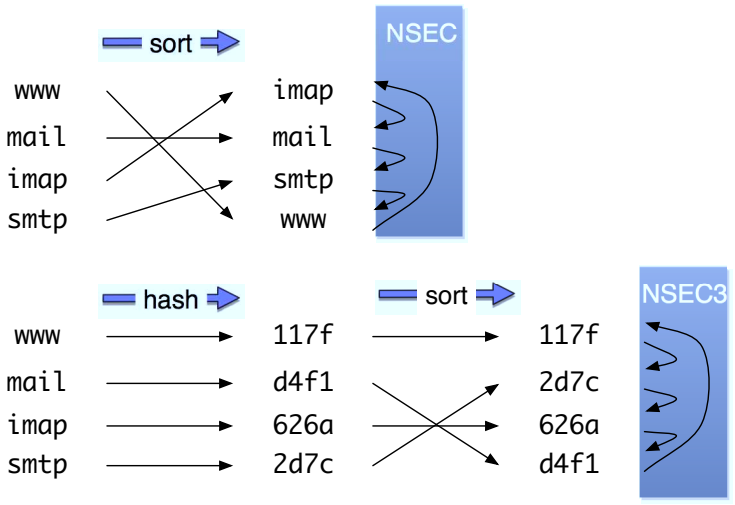
- DNSSEC
  - Uses asymmetric public key encryption
  - At least one key, usually at least two (ZSK, KSK)
  - Adds keys, signatures and other data to zone
    - Zone increases in size
  - New DNS resource records
  - Islands of trust



New DNS records

- DNSKEY
  - Public key
  - Key algorithm and data
- DS
  - Signature of the delegated zone
  - Contains key tag and hash
  - Located in parent zone
- RRSIG
  - Signature of an RRset
  - Valid for a particular time only (inception, expiry)
- NSEC/NSEC3
  - Prove non-existence (NXDOMAIN)

NSEC vs NSEC3



NSEC vs NSEC3

- NSEC
  - Does ldap.aa.net exist?
    - Nothing between "imap" and "mail"

```
$ dig +dnssec ldap.aa.net
imap.aa.net.  7200 IN NSEC mail.aa.net. A RRSIG NSEC
```

- NSEC3
  - Same question
    - Hash H("ldap") is "de16"
    - There is nothing between "626a" and "d4f1"

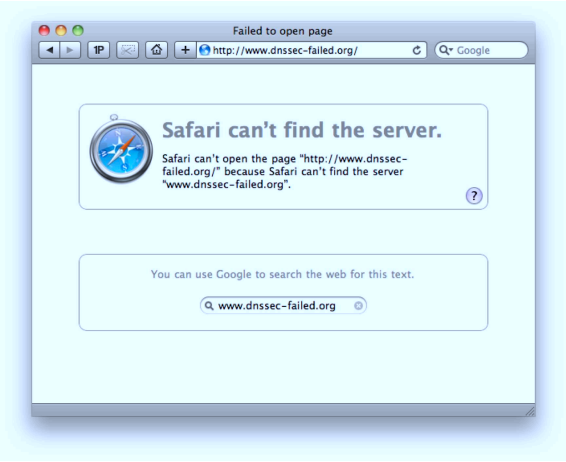
```
$ dig +dnssec ldap.aa.net
626A.aa.net. 7200 IN NSEC3 1 0 10 5AD4B3 D4F1 A RRSIG
```

Signing and validation

- Signing
  - Create keys and add to zone
  - Sign zone
  - Enable DNSSEC and load signed zones
  - Submit DS-RR to parent zone
  - Alternatively: use DLV
- Validation
  - Configure trust anchor
  - Enable DNSSEC
- Key rollovers

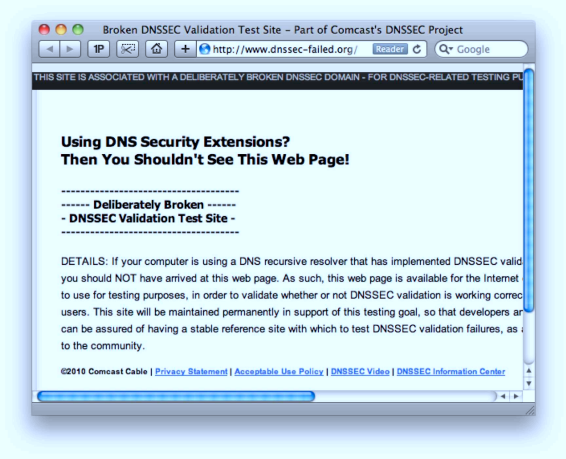
Problem: At work

- At $WORK resolution doesn't work; validating resolver



No problem: At home

- At home it works; ISP doesn't (yet) do DNSSEC



Proof

- Does it exist or doesn't it?
  - Validating query

```
$ dig +dnssec www.dnssec-failed.org
;; ->>HEADER<<- opcode: QUERY, status: SERVFAIL
;; flags: qr rd ra; QUERY: 1, ANSWER: 0
```

  - Checking Disabled

```
$ dig +cd +dnssec www.dnssec-failed.org
;; ->>HEADER<<- opcode: QUERY, status: NOERROR
;; flags: qr rd ra cd; QUERY: 1, ANSWER: 2
;; ANSWER SECTION:
www.dnssec-failed.org. 5620  IN A 68.87.64.48
```

Proof (2)

$ dig +cd +dnssec +multiline www.dnssec-failed.org

```
;; flags: qr rd ra cd; QUERY: 1, ANSWER: 2
;; ANSWER SECTION:
www.dnssec-failed.org.  3202 IN A 68.87.64.48
www.dnssec-failed.org.  4751 IN RRSIG A 5 3 7200
     20090201000000 (
     20090101000000 48621 dnssec-failed.org.
     gM8IbzE3N4xx4DQog+W2UvY+BwnLIJojFmuQUdUb7FAm
     wtD3k673q+005FDCW8xf88b+9QtvslrpNyi5ZLUq4v9k
     Xdya9Je0O2ByYjfrgjYqk4Qu37lfPe+iGvl9aSSMyGeu
     UHv9NWWY10nXjCp2rTdCSpXc7xt3CSMW7pFNFg0= )
```

Firefox

- Firefox add-on: DNSSEC Validator
  - https://addons.mozilla.org/en-US/firefox/addon/64247/

- Check: DNSSEC or not?
  - http://dnssec-or-not.org/
  - http://dnssectest.sidn.nl/

Applications for DNSSEC

- Interesting new uses for DNS now that it's secure
  - DNS-based Authentication of Named Entities (dane)
    `https://datatracker.ietf.org/wg/dane/charter/`
  - SSL certificate validation and DNSSEC (also: Phreeload)
    `http://mens.de/:/bo`
  - SSHFP
    `http://mens.de/:/bt`

DNSSEC Servers

- Authoritative
  - NSD
  - BIND
  - PowerDNS 3.0
- Recursors
  - Unbound
  - BIND

Signing tools

- BIND Utilities
  `dnssec-keygen, dnssec-signzone, dnssec-dsfromkey, ...`
- BIND automatic
  `auto-dnssec maintain;`
- ZKT (Zone Key Tool)
  - "wrapper" commands + config
  - Key-management
- OpenDNSSEC
  - black box, HSM, Signer, Auditor
- PowerDNS

Implementation: Decisions, decisions

- Key policies
  - How many? How large? Which algorithm?
  - How long should signatures be valid?
  - HSM?
- Tools
  - Which tools?
- Test implementation
- Procedures
  - Key rollovers
  - Emergency rollover
  - DLV?
  - Monitoring
- Validation on recursive caches?
  - BIND, Unbound

Thank you

Questions?

Whoami

```
$ dig 1.1.0.3.3.0.8.1.7.1.9.4.e164.arpa naptr

;; ANSWER SECTION:
1.1.0.3.3.0.8.1.7.1.9.4.e164.arpa. 3575  IN NAPTR 3 10 "u" "E2U+http" "!^.*$!http:mens.de!" .
1.1.0.3.3.0.8.1.7.1.9.4.e164.arpa. 3575  IN NAPTR 3 20 "u" "E2U+http" "!^.*$!http:blog.fupps.com!" .
1.1.0.3.3.0.8.1.7.1.9.4.e164.arpa. 3575  IN NAPTR 4 10 "u" "E2U+mailto" "!^.*$!mailto:jp@mens.de!" .
1.1.0.3.3.0.8.1.7.1.9.4.e164.arpa. 3575  IN NAPTR 1 10 "u" "E2U+sip" "!^.*$!sip:5552064@sipgate.de!" .
1.1.0.3.3.0.8.1.7.1.9.4.e164.arpa. 3575  IN NAPTR 2 10 "u" "E2U+tel" "!^.*$!tel:+491718033011!" .
```