DNSSEC par l'exemple

Francis.Dupont@fdupont.fr

OSSIRB

23 avril 2009

Plan

- Le DNS
- Les (autres) mécanismes de sécurité du DNS
- DNSSEC
- Problème de la délégation (DS)
- Problème de la négation (NSEC/NSEC3)
- Problème des comptes-rendus
- Perspectives

Le DNS(1)

- Nommage hiérarchique : domaines et zones
- Serveurs “authoritative”, caches/récursifs et clients/“resolvers”

le DNS(II)

- CNAME : indirection au niveau feuille
- wildcards (*.foo.bar) : en fait des défauts

```
[Guinness:~] dupont% dig cvs.isc.org

; <<>> DiG 9.4.2-P2 <<>> cvs.isc.org
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 55272
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;cvs.isc.org.                   IN      A

;; ANSWER SECTION:
cvs.isc.org.            43200   IN      CNAME   nexus.isc.org.
nexus.isc.org.          43200   IN      A       204.152.184.13

;; Query time: 477 msec
;; SERVER: 89.2.0.1#53(89.2.0.1)
;; WHEN: Sun Apr 19 10:37:03 2009
;; MSG SIZE  rcvd: 65

[Guinness:~] dupont%
```

```
[Guinness:~] dupont% dig this-name-does-not-exit.kr

; <<>> DiG 9.4.2-P2 <<>> this-name-does-not-exit.kr
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 58754
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;this-name-does-not-exit.kr.    IN      A

;; ANSWER SECTION:
this-name-does-not-exit.kr. 1800 IN     A       222.231.8.226

;; Query time: 41 msec
;; SERVER: 89.2.0.1#53(89.2.0.1)
;; WHEN: Sun Apr 19 10:54:25 2009
;; MSG SIZE  rcvd: 60

[Guinness:~] dupont%
```

le DNS(III)

- 4 types de réponses :
  - réponse standard
  - NXDOMAIN : le nom n'existe pas
  - NODATA (condition): le nom existe mais n'a pas de Resource Record du bon type
  - Referral

```
[Guinness:~] dupont% dig www.example.com

; <<>> DiG 9.4.2-P2 <<>> www.example.com
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 38485
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;www.example.com.               IN      A

;; ANSWER SECTION:
www.example.com.        172800  IN      A       208.77.188.166

;; Query time: 259 msec
;; SERVER: 89.2.0.1#53(89.2.0.1)
;; WHEN: Sat Apr 18 22:27:59 2009
;; MSG SIZE  rcvd: 49

[Guinness:~] dupont%
```

```
[Guinness:~] dupont% dig ww.example.com

; <<>> DiG 9.4.2-P2 <<>> ww.example.com
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 17556
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 0

;; QUESTION SECTION:
;ww.example.com.                        IN      A

;; AUTHORITY SECTION:
example.com.            86400   IN      SOA     dns1.icann.org. hostmaster.icann
.org. 2007051703 7200 3600 1209600 86400

;; Query time: 231 msec
;; SERVER: 89.2.0.1#53(89.2.0.1)
;; WHEN: Sat Apr 18 22:39:34 2009
;; MSG SIZE  rcvd: 93

[Guinness:~] dupont%
```

```
[Guinness:~] dupont% dig -t txt www.example.com

; <<>> DiG 9.4.2-P2 <<>> -t txt www.example.com
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 57979
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 0

;; QUESTION SECTION:
;www.example.com.               IN      TXT

;; AUTHORITY SECTION:
example.com.            86400   IN      SOA     dns1.icann.org. hostmaster.icann
.org. 2007051703 7200 3600 1209600 86400

;; Query time: 54 msec
;; SERVER: 89.2.0.1#53(89.2.0.1)
;; WHEN: Sat Apr 18 22:43:26 2009
;; MSG SIZE  rcvd: 94

[Guinness:~] dupont%
```

```
[Guinness:~] dupont% dig www.example.com @f.gtld-servers.net

; <<>> DiG 9.4.2-P2 <<>> www.example.com @f.gtld-servers.net
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 45293
;; flags: qr rd; QUERY: 1, ANSWER: 0, AUTHORITY: 2, ADDITIONAL: 2
;; WARNING: recursion requested but not available

;; QUESTION SECTION:
;www.example.com.               IN      A

;; AUTHORITY SECTION:
example.com.            172800  IN      NS      a.iana-servers.net.
example.com.            172800  IN      NS      b.iana-servers.net.

;; ADDITIONAL SECTION:
a.iana-servers.net.     172800  IN      A       192.0.34.43
b.iana-servers.net.     172800  IN      A       193.0.0.236

;; Query time: 201 msec
;; SERVER: 192.35.51.30#53(192.35.51.30)
;; WHEN: Sat Apr 18 22:47:02 2009
;; MSG SIZE  rcvd: 113

[Guinness:~] dupont%
```

Résolution

- En pratique : utilisation d'un serveur cache (aka récursif) :"stub resolver"
- En théorie : suivre les referrals depuis la racine

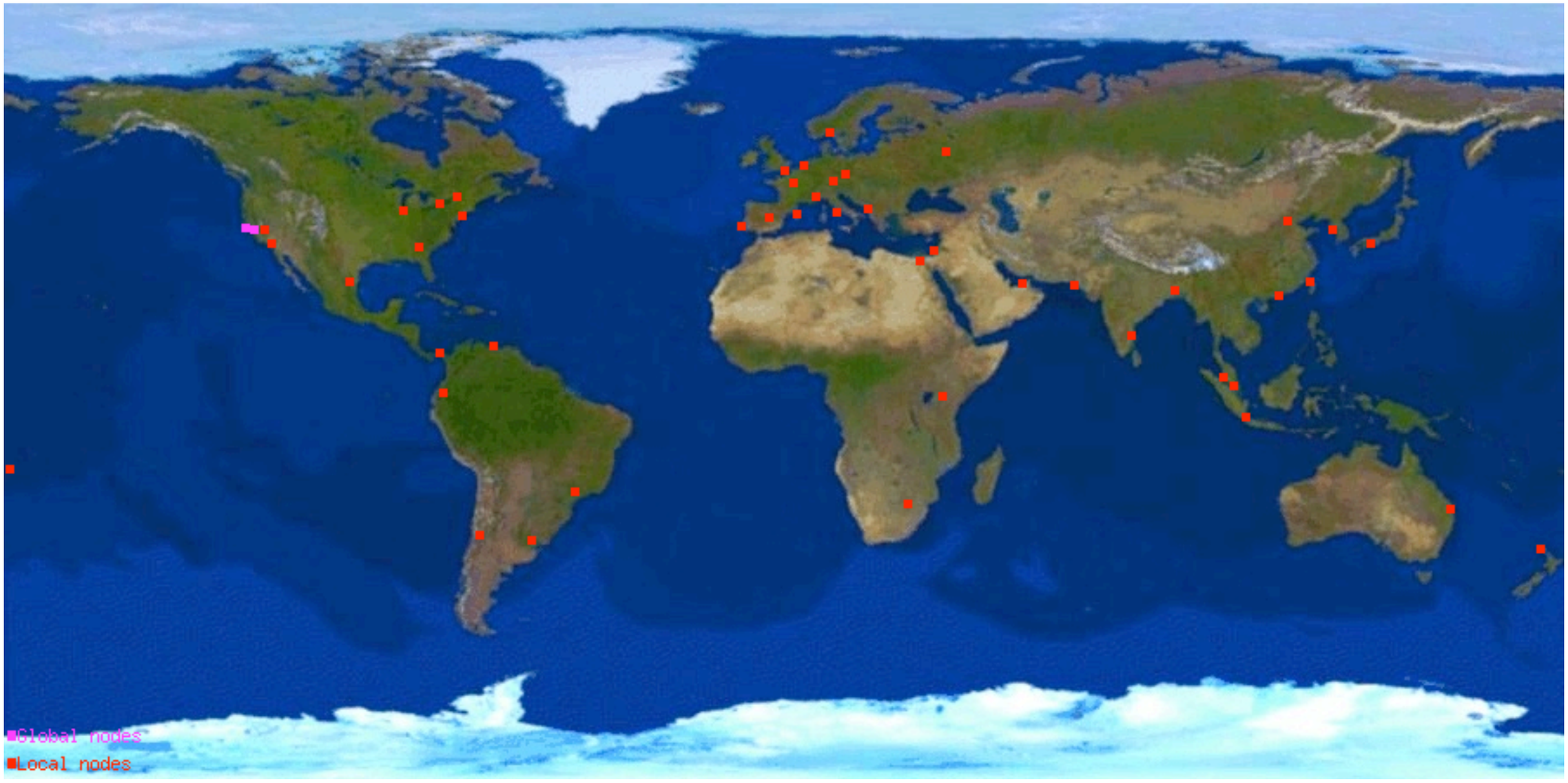
```
[Guinness:/tmp] dupont% cat trace

; <<>> DiG 9.6.0rc1 <<>> +trace -t txt test.dnssec-tools.org
;; global options: +cmd
.                       371113  IN      NS      a.root-servers.net.
.                       371113  IN      NS      g.root-servers.net.
.                       371113  IN      NS      l.root-servers.net.
.                       371113  IN      NS      i.root-servers.net.
.                       371113  IN      NS      f.root-servers.net.
.                       371113  IN      NS      d.root-servers.net.
.                       371113  IN      NS      b.root-servers.net.
.                       371113  IN      NS      m.root-servers.net.
.                       371113  IN      NS      j.root-servers.net.
.                       371113  IN      NS      h.root-servers.net.
.                       371113  IN      NS      c.root-servers.net.
.                       371113  IN      NS      k.root-servers.net.
.                       371113  IN      NS      e.root-servers.net.
;; Received 449 bytes from 212.27.40.240#53(212.27.40.240) in 51 ms

org.                    172800  IN      NS      A0.ORG.AFILIAS-NST.INFO.
org.                    172800  IN      NS      B0.ORG.AFILIAS-NST.org.
org.                    172800  IN      NS      D0.ORG.AFILIAS-NST.org.
org.                    172800  IN      NS      B2.ORG.AFILIAS-NST.org.
org.                    172800  IN      NS      A2.ORG.AFILIAS-NST.INFO.
org.                    172800  IN      NS      C0.ORG.AFILIAS-NST.INFO.
;; Received 441 bytes from 128.8.10.90#53(d.root-servers.net) in 141 ms

dnssec-tools.org.       86400   IN      NS      ns1.dnssec-tools.org.
dnssec-tools.org.       86400   IN      NS      ns4.dnssec-tools.org.
;; Received 107 bytes from 2001:500:f::1#53(D0.ORG.AFILIAS-NST.org) in 209 ms

test.dnssec-tools.org.  86400   IN      TXT     "DNSSEC-TOOLS test zone for test
.dnssec-tools.org"
test.dnssec-tools.org.  86400   IN      NS      dns1.test.dnssec-tools.org.
test.dnssec-tools.org.  86400   IN      NS      dns2.test.dnssec-tools.org.
;; Received 170 bytes from 76.216.12.217#53(ns4.dnssec-tools.org) in 215 ms

[Guinness:/tmp] dupont%
```

Sécurité des transactions

- Nécessité pour les “dynamic updates” et les transferts de zone
- TSIG, SIG(0), TKEY
- IPsec, SSL/TLS, ...

Résistance au DoS

- Anycasting (exemple du serveur racine F)


Global nodes
Local nodes

DNSSEC

- Idée : signature des données (RRset), délégation des zones == chaînage des clés/signatures
- initialement KEY, SIG, NXT, maintenant DNSKEY, RRSIG, NSEC/NSEC3, DS

DNSKEY

- clé publique RSA (MD5, SHA-1), DSA
- flags (SEP), protocole (obsolète), algorithme, valeur (clé publique)
- (implicite) “key tag”

RRSIG

- signature d'un RRset
- type couvert, algorithme, nombre d'étiquettes, TTL d'origine, dates de début et de fin de validité, "key tag", nom du signataire, valeur (signature)

NSEC

- Preuve d'existence/non-existence
- nom suivant, types existant

DS

- Chaînage (hachage SHA-1/SHA-256)
- “key tag”, algorithme, “digest type”, valeur (hachage du DNSKEY RR)
- Appartient à la zone parente (exception)

NSEC3

- Variante de NSEC ne permettant pas le parcours de zone
- hachage itéré avec sel : espace indépendant de noms
- bit “optout”
- NSEC3PARAM

```
[Guinness:~] dupont% dig +dnssec www.isc.org @ams.sns-pb.isc.org

; <<>> DiG 9.4.2-P2 <<>> +dnssec www.isc.org @ams.sns-pb.isc.org
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 23644
;; flags: qr aa rd; QUERY: 1, ANSWER: 2, AUTHORITY: 5, ADDITIONAL: 11
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 4096
;; QUESTION SECTION:
;www.isc.org.                   IN      A

;; ANSWER SECTION:
www.isc.org.            600     IN      A       149.20.64.42
www.isc.org.            600     IN      RRSIG   A 5 3 600 20090518130827 2009041
8130827 50082 isc.org. LehVZh0PT+J/10iU9VXbpxev3+/tqSyzBGuRvI0DXDOx7EFMZVO+7njW
Q1qFfMKgzDknI6cFafDpwRVPDnlhtT0ejt6FofCosWv7Vgv7JP0a0ozN csWcCcG5hQXMtTr5B9GkhYI
ucdv+X7aFjba8vQPpN8ogKbS4wB5W3s4u j4c=

;; AUTHORITY SECTION:
isc.org.                43200   IN      NS      ord.sns-pb.isc.org.
isc.org.                43200   IN      NS      ns-ext.nrt1.isc.org.
isc.org.                43200   IN      NS      ams.sns-pb.isc.org.
isc.org.                43200   IN      NS      sfba.sns-pb.isc.org.
isc.org.                43200   IN      RRSIG   NS 5 2 43200 20090518130827 2009
0418130827 50082 isc.org. tYm/LNL0FBcLJ7BxUV9kKiD+ZKto7b8KF223K4bEIQN1tbrwb6BIw6
Uj 8GdOFeL4DKb6xWlp1vWwbCCM0p9qR8CZFqr8r0D1Eiywx7o8fi44ojJx Gdr2usDihSCSYEnXwOIV
WMt66AVrCvVEuGptb/l0jluBfuilx8tkZyl/ 4oU=

;; ADDITIONAL SECTION:
ams.sns-pb.isc.org.     43200   IN      A       199.6.1.30
ord.sns-pb.isc.org.     43200   IN      A       199.6.0.30
sfba.sns-pb.isc.org.    43200   IN      A       149.20.64.3
sfba.sns-pb.isc.org.    43200   IN      AAAA    2001:4f8:0:2::19
ns-ext.nrt1.isc.org.    3600    IN      A       192.228.90.19
ams.sns-pb.isc.org.     43200   IN      RRSIG   A 5 4 43200 20090518130827 20090
418130827 50082 isc.org. F4ocgS7zfWpAc/Lyub8ANnY05mGJHJQCWP0DV872E70NrlSr2RGRjmw
k qTtTI+AJzRuIRVqs/mk+5xicyJ3UGsFJJvDXiabwoFhWbo+bXN6zgLw8 dh+V+XmWL8PjkoltkEjcK
OxV3RCXKh60rDyKUYm/shuGHDyWLZST9Mzk 2lM=
```

```
[Guinness:~] dupont% dig +dnssec ww.isc.org @ams.sns-pb.isc.org

; <<>> DiG 9.4.2-P2 <<>> +dnssec ww.isc.org @ams.sns-pb.isc.org
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 42558
;; flags: qr aa rd; QUERY: 1, ANSWER: 0, AUTHORITY: 6, ADDITIONAL: 1
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 4096
;; QUESTION SECTION:
;ww.isc.org.                    IN      A

;; AUTHORITY SECTION:
isc.org.                3600    IN      SOA     ns-int.isc.org. hostmaster.isc.o
rg. 2009041804 7200 3600 24796800 3600
isc.org.                3600    IN      RRSIG   SOA 5 2 43200 20090518130827 200
90418130827 50082 isc.org. EC4fT+rN2LiimDM4aM6GLBmUGmEUSpx6pW3Ucn2EYwz3Mk7E1EG+K
3tc KeFowV7xwmei3nnGIVW50xXIQM/hjndI65tRvp+shj7jphJF6nlXtLg6 QprnGddUQkrswAFLTwP
AI3kJlp0c/CEL3UkX7sABdTYAue8K0UBpR/cZ 4MM=
isc.org.                3600    IN      NSEC    _kerberos.isc.org. A NS SOA MX T
XT AAAA NAPTR RRSIG NSEC DNSKEY
isc.org.                3600    IN      RRSIG   NSEC 5 2 3600 20090518130827 200
90418130827 50082 isc.org. kXEt+XjdrogLdsBcuEIGdCMhA6e3UgkzZznPmXUDxhF2qI+wBZhsc
qQk t2c0Oe+YBq2/uUmZliwzlVkTQc3TmHvFQ0DipPTODoWKzoOE351fqrps soxbBtfHrhiX2fxt1Bu
49fQEPXZGWtSldS/z5DaymYzp8n6vlrvpAikj tHw=
wolfgang.isc.org.       3600    IN      NSEC    www.isc.org. A RRSIG NSEC
wolfgang.isc.org.       3600    IN      RRSIG   NSEC 5 3 3600 20090518130827 200
90418130827 50082 isc.org. pMQ3FeK7MBhTYAhYgB4mT09j5QEiP3Fes+EXqrLoaePKuxmpARvba
xKY hQTqCu4Q5EzI1a5ua/wSYJ6QrgUX3unATvFU13vIsFypSZ6nmzoo//12 E98Lvu0k9kymDEueXyR
X4RiId2NTF5tVm+baPVzfoQJurebbQVUetSk1 QWw=

;; Query time: 52 msec
;; SERVER: 199.6.1.30#53(199.6.1.30)
;; WHEN: Sat Apr 18 23:57:54 2009
;; MSG SIZE  rcvd: 676

[Guinness:~] dupont%
```

```
[Guinness:~] dupont% dig +dnssec -t txt www.isc.org @ams.sns-pb.isc.org

; <<>> DiG 9.4.2-P2 <<>> +dnssec -t txt www.isc.org @ams.sns-pb.isc.org
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 51095
;; flags: qr aa rd; QUERY: 1, ANSWER: 0, AUTHORITY: 4, ADDITIONAL: 1
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 4096
;; QUESTION SECTION:
;www.isc.org.                   IN      TXT

;; AUTHORITY SECTION:
isc.org.                3600    IN      SOA     ns-int.isc.org. hostmaster.isc.o
rg. 2009041804 7200 3600 24796800 3600
isc.org.                3600    IN      RRSIG   SOA 5 2 43200 20090518130827 200
90418130827 50082 isc.org. EC4fT+rN2LiimDM4aM6GLBmUGmEUSpx6pW3Ucn2EYwz3Mk7E1EG+K
3tc KeFowV7xwmei3nnGIVW50xXIQM/hjndI65tRvp+shj7jphJF6nlXtLg6 QprnGddUQkrswAFLTwP
AI3kJlp0c/CEL3UkX7sABdTYAue8K0UBpR/cZ 4MM=
www.isc.org.            3600    IN      NSEC    www-int.isc.org. A AAAA RRSIG NS
EC
www.isc.org.            3600    IN      RRSIG   NSEC 5 3 3600 20090518130827 200
90418130827 50082 isc.org. JQskKnI9lofjcyYUrP69DPP4S5hub5tj0HcZ2CdrS4c8gP4S4HM/1
aAD o9kv0viEkJELnS9o2gMkHDXzsDRJbxEWTDIh5DZy5B9TATRq0LymhtTN 2xeTY6tw5VPtdiitaIn
1ui/G99KcPkv9BHxV8hlSC87pQftXHoirE91f Egs=

;; Query time: 41 msec
;; SERVER: 199.6.1.30#53(199.6.1.30)
;; WHEN: Sun Apr 19 00:00:36 2009
;; MSG SIZE  rcvd: 465

[Guinness:~] dupont%
```

```
[Guinness:~] dupont% dig +dnssec www.afasi.ac.se @a.ns.se

; <<>> DiG 9.4.2-P2 <<>> +dnssec www.afasi.ac.se @a.ns.se
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 42004
;; flags: qr rd; QUERY: 1, ANSWER: 0, AUTHORITY: 4, ADDITIONAL: 1
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 4096
;; QUESTION SECTION:
;www.afasi.ac.se.               IN      A

;; AUTHORITY SECTION:
afasi.ac.se.            86400   IN      NS      dns9.telia.com.
afasi.ac.se.            86400   IN      NS      dns10.telia.com.
afasi.ac.se.            7200    IN      NSEC    annova.ac.se. NS RRSIG NSEC
afasi.ac.se.            7200    IN      RRSIG   NSEC 5 3 7200 20090423225429 200
90418181804 19176 se. VzFnmZb5JQO1gE2/ShRgTKv1xLjgiMOUNdNCKAqaY3ChpofoZL6yNsY6 +
bnJlVmgTSydWocBtxfupOTaQpx6KUlQK8OrcdfieybArn8e0J9Jf5tY VoKExV4aCFZFn25jfwaJSkgJ
ReUIgzD8gZ+Y1NUAFCUOHw7V2SrvijLg 2rk=

;; Query time: 66 msec
;; SERVER: 192.36.144.107#53(192.36.144.107)
;; WHEN: Sun Apr 19 00:08:57 2009
;; MSG SIZE  rcvd: 288

[Guinness:~] dupont%
```

```
[Guinness:~] dupont% dig +dnssec nic.se @a.ns.se

; <<>> DiG 9.4.2-P2 <<>> +dnssec nic.se @a.ns.se
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 40319
;; flags: qr rd; QUERY: 1, ANSWER: 0, AUTHORITY: 6, ADDITIONAL: 5
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 4096
;; QUESTION SECTION:
;nic.se.                                IN      A

;; AUTHORITY SECTION:
nic.se.                 86400   IN      NS      ns3.nic.se.
nic.se.                 86400   IN      NS      ns.nic.se.
nic.se.                 86400   IN      NS      ns2.nic.se.
nic.se.                 3600    IN      DS      16696 5 1 EF5D421412A5EAF1230071
AFFD4F585E3B2B1A60
nic.se.                 3600    IN      DS      16696 5 2 40079DDF8D09E7F10BB248
A69B6630478A28EF969DDE399F95BC3B39 F8CBACD7
nic.se.                 3600    IN      RRSIG   DS 5 2 3600 20090425113307 20090
418181804 19176 se. QzO9GMqy9fS1orNfiiZTWUxcz8AMmxqoRTgHxFL8BVexwGIGnIf4yhJ1 NU/
cIYVhTTjRP6wp7S7/FPeduzSfXhtjpS1spTnek6YJbTseaLrfx9u1 XivnjxnbsY2hMaxaZ//zi090hB
sUYUR0b7DCsJVBwZ5uNz250ge+0vzZ 2Zw=

;; ADDITIONAL SECTION:
ns.nic.se.              86400   IN      A       212.247.7.228
ns.nic.se.              86400   IN      AAAA    2a00:801:f0:53::53
ns2.nic.se.             86400   IN      A       194.17.45.54
ns3.nic.se.             86400   IN      A       212.247.3.83

;; Query time: 52 msec
;; SERVER: 192.36.144.107#53(192.36.144.107)
;; WHEN: Sun Apr 19 00:19:06 2009
;; MSG SIZE  rcvd: 410

[Guinness:~] dupont%
```

```
[Guinness:~] dupont% dev/b/bin/dig/dig +dnssec foobar.gov @a.gov.zoneedit.com

; <<>> DiG 9.7.0pre-alpha <<>> +dnssec foobar.gov @a.gov.zoneedit.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 53190
;; flags: qr aa rd; QUERY: 1, ANSWER: 0, AUTHORITY: 8, ADDITIONAL: 1
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 4096
;; QUESTION SECTION:
;foobar.gov.                    IN      A

;; AUTHORITY SECTION:
gov.                    86400   IN      SOA     A.GOV.ZONEEDIT.COM. govcontact.Z
ONEEDIT.COM. 1240088462 3600 900 1814400 86400
gov.                    86400   IN      RRSIG   SOA 7 1 259200 20090423200103 20
090418200103 31802 gov. Q1vbeqD4O+mCnybGtp66elrXbMPN6fctivDc4RfG/31qNppPcSiOEE79
 q66Cq6kv0tEA6BAHIkLKd9MhTDDBBtzMcbaoVivzX7ZuITsRVGQK5HZo 8KjV9641+lzBJuyoch+kG/
YJW6PI+J3HqLa0bkJOkqHyXcqLM8cQWo2q OjqH+yS4qF3Sz41ripC0tIbD4RpQS/UsPNOS9Gc22otBa
CgAkVxZtA2i 9xk1dvAqg9EvizDcrvZenf8a5x09LMnTSQ2z7sHIVX8HtmejL2sIl2kj C6jAhswAQhV
ky2HsDMfHdGFSCF+aZRLTSeWZ7c6Sw+WVx2VBNMSiXcym lwuqyw==
VVSOMCNUB7A79EALVJEH4VN12192C715.gov. 86400 IN NSEC3 1 0 10 ABAB 0002H1U5Q5HGQCI
TMSB0QRETCK0N6FLT NS SOA RRSIG DNSKEY NSEC3PARAM
VVSOMCNUB7A79EALVJEH4VN12192C715.gov. 86400 IN RRSIG NSEC3 7 2 86400 20090423200
103 20090418200103 31802 gov. Lg/94ECEayl/964qjXxwEINavEbvKdRypk86N7VMeOILM0htUd
A8Zfby 53VEbWbKFd/7SFbJLRYNBEfxT2mUIoWoYQgiGaup9FAyQRu2OBsFZC3p PXx65UDFX0qrCzV5
0bdPR0ONkwHtn74LCVhFPn3YJa7/KEOBdJCbjHYj jsW3Ud0HYheTBHO1cHg8OOAMbABfsLi9yrdQ5sN
0371j8y/xHTsldnyB NjoJgdN2GBCBlHSgJmlxGRo2R03UzmqGi7ILqPo0g0MAT6YPieHOw4p7 O1tIS
lmCTQXswy6M8vadNWXkWuuj7+odN3t9B+1HvnnPsU7uZrbV1Fe3 M673aA==
6ESUOQLGN6O4L45P4KLVKQEO1BKK7CSH.gov. 86400 IN NSEC3 1 0 10 ABAB 6F45H2C48EG2U4V
EIKL6DJ5JSJFPGPSB NS
6ESUOQLGN6O4L45P4KLVKQEO1BKK7CSH.gov. 86400 IN RRSIG NSEC3 7 2 86400 20090423200
103 20090418200103 31802 gov. DW3UA1yJ6CxlsC/rX+PjTaSinuKZLPVHsR0Gn9WI9QMO0R9tKU
4ddw0B zDqZb3NExR7R/EeBM71IMobbeUwPqs2r7FTWkW6wpj1p3h66FOu6XlKG wnkwXBaC+hHpDdQT
Sa6/St1iLFxYkbSQLN8u8XPOnPmKawej7OF2465A 1nRushPMqTDyRiysqX2ccu7iEo2dJc25QtL/+w3
lMK5u+04/ZDsuz6Sh U9jZIniQr/69uuXC4XM0uglgfMTqzAs9MKtKMPBWlcKmtVxIFXxiWdgz NEW1G
/EH+CRsPGgcHFWzIRBfQ+CFbluGWbsAVebQA1AdejvorUBFd1Ge mwtPyQ==
RGUV32S6M8P4NA9SPC8R07OAARC29LUL.gov. 86400 IN NSEC3 1 0 10 ABAB RH0C9GRADSDFR8V
387EA61I4H1V1GJU4 NS
RGUV32S6M8P4NA9SPC8R07OAARC29LUL.gov. 86400 IN RRSIG NSEC3 7 2 86400 20090423200
103 20090418200103 31802 gov. l+doSZC91s/Eh1mdXQJTYS2G0J/gDX569UFH9h2Br7lFCEtiF/
gvj214 pmpRAlyEkgnQyj2p+jZWtESaloNqiMxAD7di3QRU54mfbA7dTWR+xiaK CIzOXkbOohMGGzqy
ZB9C5KiPFzUtwkZfU0uYyIUVFm6oatkup+OvPl2n IjVcxgMz49oZJv3KuhACGGzNOwgH8Bo0o3eLo4u
HUVlGVm0lkMXRYaNd K68qkNbTURAxkQ754IJnHaLYdC2rjLbbMKhbqfxp3vn9M02p3S0qy60a TlQeW
d9bB/Z94Vu3pXwquxLTLUM5sZhY3hINGrie3pTCMNmXoaCGAVSd 9Gotig==

;; Query time: 207 msec
;; SERVER: 216.55.155.29#53(216.55.155.29)
;; WHEN: Sun Apr 19 11:39:35 2009
;; MSG SIZE  rcvd: 1502

[Guinness:~] dupont%
```

```
[Guinness:~] dupont% dev/b/bin/tools/nsec3hash ABAB 1 10 gov
VVSOMCNUB7A79EALVJEH4VN12192C715 (salt=ABAB, hash=1, iterations=10)
[Guinness:~] dupont% dev/b/bin/tools/nsec3hash ABAB 1 10 foobar.gov
6F41V8DHP5ETMABLGN76A58L4GO66300 (salt=ABAB, hash=1, iterations=10)
[Guinness:~] dupont% dev/b/bin/tools/nsec3hash ABAB 1 10 '*.gov'
RH098M4V941H6QNB9S5EHBI2GAJOKA5U (salt=ABAB, hash=1, iterations=10)
[Guinness:~] dupont%
```

Délégation

- À qui appartient l’“apex”/”delegation point”/”zone cut” d’une zone ?
- Réponse : au fils sauf pour les DS RR

(Non-)Existence

- NODATA : liste des types existant
- NXDOMAIN : nom dans un espace couvert par un NSEC
- Problème des wildcards :“closest encloser”
- Pire avec NSEC3 :“closest provable encloser”,“next closer”,“empty non-terminal”, etc

Comptes-rendus

- Nouveaux cas, par exemple “provable insecure”
- Erreurs cryptiques : exemple “not insecure” (changé en “insecurity proof failed: got insecure response; could not prove it was valid”)
- Pas d’API standard, cas particuliers pour chaque application ?

Validation

- bit DO (dans EDNS0) :“DNSSEC capable”
- Not-validating security-aware resolver: validating caching server + bit AD + communications protégées (Microsoft W7)
- Validating resolver (+ bit CD) : recherche des DNSKEY/DS jusqu’à une clé connue (aka trust anchor aka security entry point)

```
[Guinness:/tmp] dupont% cat sigchase
;; RRset to chase:
test.dnssec-tools.org.  86400   IN      TXT     "DNSSEC-TOOLS test zone for test
.dnssec-tools.org"


;; RRSIG of the RRset to chase:
test.dnssec-tools.org.  86400   IN      RRSIG   TXT 5 3 86400 20090426155658 200
90327155658 19442 test.dnssec-tools.org. xQT1wU0hLybQ/NhcPDoR+XdBqpFu813RahwkdT8
BRfrnRDjEWMKF5Q+r AR9BfyRjqp9xVEoXI3Y71Yxklz4oELdVpp7R+qf0SOM0bf5bupV++rrC MyNFu
vVABgCg1DiwaIWTfmVsAZYCJSmz2k+sHoXIcU2jUDHu9i4wtXha da4=



Launch a query to find a RRset of type DNSKEY for zone: test.dnssec-tools.org.

;; DNSKEYset that signs the RRset to chase:
test.dnssec-tools.org.  86400   IN      DNSKEY  257 3 5 AQPUlH65Otuo6toxYX2zHCwd
ojmAKFa9gobYWrNEojKQAWJuvGMd4okT nlOJTL0hBWKC4Uhf40ePpDR8QJayeI/eZg29UZLMBleZ96a
0mSo/JU4S q3G06X9d5Z01EVCvTkJUHHEvvmzZhBsO+43NcWYrSUoXX1JbXs9QKuO1 BLPHuS5G/UfEs
yVonfl39dGrEput1gDWxIvov2UENM2eX0LE5ZIyGiX2 uDdN4SVIa0Rd+F2pSCiddE1bYxIi2IlW6bpe
im+mdC1BDJkEB70+ekeB R3as5D339z+9KeMyZgPs82SAQswbGdZvkWL8mgSdbf6DiuTkkNIUzbS/ 6f
xlQO/GOdq0NlTr28sW4Byj9gkpb2Clbqog72yJJ3s5CV4LGZ1jtpno FcsKwMlLnOj0X+L2iY7Spe5M9
D59Jqxl9cAWjATsSXG5TvCUNBT2Eh6J w7OimThJe4pUmFxGqhplPqs2dlnDgfcuVNf9lwa36Re7pUt+
FlT0A9FI Wk4utfUgZO3eWnKrw1Fw8QF9wKm252iscULNzKwYvfK8NGSBOfyYRvAw 7ZnAoxMKFIOLq3
W8IsFjti5dLhLYWpFEGZOT+eDc/lPhyaEsmsjHQnEE yj4TmomV8n91s3H8IbrKu0cdIH1/k5iu+sLi9
EIAprOnxrxO+tHDiEZU oimBRFtETCcmsQ==
test.dnssec-tools.org.  86400   IN      DNSKEY  257 3 5 AQPbjy5TVjquKVVTYjCYOHUH
orMbj0LxpVSF7/QAJTi+Y6hcMoQrWjrl aLSLNNa0wFDMxXnnlD/KYj9GtX5Vq/dP/glW73lOU5CXrwX
ujvyXp7Wh vu8F2jLJEUoU1bZD12ZfGTmnflYblAJz3lPNy5ZHiiSicD+7+uW0rSSX LLEwHd007jcEM
grH6B/jjk3bCHnXnQMclTEx2k/dKqcs+Ohrhc98oK8r DQz+Rq+uTOoscWHuKy8aORYDXCqbUxS5VwIJ
xgLTC7DQ3c3qSOIkvWdA KJJTnPabPWeELK15CIO3+uAC+oUyJ51EC2qpJlpJc6knEeCYNYZP/HBp aF
S8Vz2j
test.dnssec-tools.org.  86400   IN      DNSKEY  256 3 5 AQPXOnkFeyoD9Ypwt4rZgLoe
O6hwJtFx+k/LNqv6CMSZAsPm5mbEo3ke dYZ9RlgTr1b7qH3bso5qdYGJkz3u6j05GcoIJmwXlHQY+Nt
PtsukN/4R h+jcyX8N2WdYhYGlQZ6W25ljszZ5F3mhgnXrMz+o9S2t+l8ppM9LipPX uMhMFQ==
test.dnssec-tools.org.  86400   IN      DNSKEY  256 3 5 AQPgjVLwLeMvBCZSYvwabhRs
J0rQ5lylkc8M9OrNoR1BLDep23A1uXbY q/fV9jwjFvIcI//Y/3Hmmk87+DBvojKV5XngSi8B95wJW+w
+IEuTaTgP gFg3XiuX5LaU7G2Q6IQF2Fwpcw+gf613srYCQAk1EflwDaaC0mX64gFq q3tisQ==


;; RRSIG of the DNSKEYset that signs the RRset to chase:
test.dnssec-tools.org.  86400   IN      RRSIG   DNSKEY 5 3 86400 20090426155658
20090327155658 19442 test.dnssec-tools.org. lcOBlBr8zOV3QNqSv7wDYARaCJV2mWnX7+SW
2XUaDXZTMXXosOK/mdzg KP2C0iHCpE7wlIuxoaJ3hC0xdvG6I8vFTawInIXcJwI6cmt14hi84X8I mp
HmDzwaHAlwjM3CDe9tAmad3cJbPAC2SEzm3V+kHADwyglDXL4NTu/F 0fg=
test.dnssec-tools.org.  86400   IN      RRSIG   DNSKEY 5 3 86400 20090426155658
20090327155658 28827 test.dnssec-tools.org. haVgdOyLFERtKcI5AGIdIyv4fKYrHufyiy2s
yuIA4AYY8/T6Jodjqs57 F9KdCpS/xOdTnCD9k4TyrnazFoBPG+xaWGaOSXg7zRQYQIJ3ZlAQuOKU B9
zzpxaJOB8Psc8UK0VEXbQfsyrKYBBASL6oVOavq+/42JyimIilOuvW HUv3Ybp2oFGRJRJ1bs+K5+SLr
xzrrJx1Yroq96KtpOa07bCXZo85gY6z GpmU5wKfyjF3VyEJUewSc1pho7GYwfvAVSM/zQVD0AcybAzj
/3UspVb/ NiblRmIYmeslZTpXzcFnsUDRFPT5JjLE6cKNpGs+g1gUfbnoDmWiIBjK 1V2JIGXx9Ra0D1
1WZzOvJAIuOwhtnZ0cwflKbvO4JeTYL55d2D/KPbtu niMcUU+n2dcaSzODCRZ4Aib81VS3Y/kini5nA
```

```
[Guinness:/tmp] dupont% cat uhost
[1240128911] libunbound[29937:0] notice: init module 0: validator
[1240128911] libunbound[29937:0] notice: init module 1: iterator
[1240128911] libunbound[29937:0] info: resolving <test.dnssec-tools.org. TXT IN>
[1240128911] libunbound[29937:0] info: priming . IN NS
[1240128911] libunbound[29937:0] info: resolving <B.ROOT-SERVERS.NET. AAAA IN>
[1240128911] libunbound[29937:0] info: priming . IN NS
[1240128911] libunbound[29937:0] info: cycle detected <. NS IN>
[1240128911] libunbound[29937:0] info: resolving <G.ROOT-SERVERS.NET. AAAA IN>
[1240128911] libunbound[29937:0] info: priming . IN NS
[1240128911] libunbound[29937:0] info: cycle detected <. NS IN>
[1240128911] libunbound[29937:0] info: response for <. NS IN>
[1240128911] libunbound[29937:0] info: reply from <.> 2001:500:3::42#53
[1240128911] libunbound[29937:0] info: query response was ANSWER
[1240128911] libunbound[29937:0] info: priming successful for <. NS IN>
[1240128911] libunbound[29937:0] info: resolving <e.root-servers.net. AAAA IN>
[1240128911] libunbound[29937:0] info: resolving <c.root-servers.net. AAAA IN>
[1240128911] libunbound[29937:0] info: resolving <g.root-servers.net. AAAA IN>
[1240128911] libunbound[29937:0] info: resolving <b.root-servers.net. AAAA IN>
[1240128911] libunbound[29937:0] info: resolving <d.root-servers.net. AAAA IN>
[1240128911] libunbound[29937:0] info: resolving <i.root-servers.net. AAAA IN>
[1240128911] libunbound[29937:0] info: response for <d.root-servers.net. AAAA IN
>
[1240128911] libunbound[29937:0] info: reply from <.> 193.0.14.129#53
[1240128911] libunbound[29937:0] info: query response was ANSWER
[1240128911] libunbound[29937:0] info: response for <i.root-servers.net. AAAA IN
>
[1240128911] libunbound[29937:0] info: reply from <.> 192.5.5.241#53
[1240128911] libunbound[29937:0] info: query response was ANSWER
[1240128911] libunbound[29937:0] info: response for <g.root-servers.net. AAAA IN
>
[1240128911] libunbound[29937:0] info: reply from <.> 2001:7fd::1#53
[1240128911] libunbound[29937:0] info: query response was ANSWER
[1240128911] libunbound[29937:0] info: response for <b.root-servers.net. AAAA IN
>
[1240128911] libunbound[29937:0] info: reply from <.> 192.112.36.4#53
[1240128911] libunbound[29937:0] info: query response was ANSWER
[1240128912] libunbound[29937:0] info: response for <c.root-servers.net. AAAA IN
>
[1240128912] libunbound[29937:0] info: reply from <.> 198.41.0.4#53
[1240128912] libunbound[29937:0] info: query response was ANSWER
[1240128912] libunbound[29937:0] info: response for <e.root-servers.net. AAAA IN
>
[1240128912] libunbound[29937:0] info: reply from <.> 192.203.230.10#53
[1240128912] libunbound[29937:0] info: query response was ANSWER
[1240128912] libunbound[29937:0] info: response for <test.dnssec-tools.org. TXT
IN>
[1240128912] libunbound[29937:0] info: reply from <.> 2001:dc3::35#53
[1240128912] libunbound[29937:0] info: query response was REFERRAL
[1240128912] libunbound[29937:0] info: response for <test.dnssec-tools.org. TXT
IN>
[1240128912] libunbound[29937:0] info: reply from <org.> 199.19.57.1#53
[1240128912] libunbound[29937:0] info: query response was REFERRAL
[1240128912] libunbound[29937:0] info: resolving <ns1.dnssec-tools.org. AAAA IN>
[1240128912] libunbound[29937:0] info: resolving <ns4.dnssec-tools.org. AAAA IN>
```

Remarques

- Dépend d'EDNS0 (comme IPv6)
- NSEC3 est probablement trop compliqué pour des utilisateurs lambda mais a été exigé par des gérants de TLD...
- RSA / SHA-2 en cours de standardisation
- Quelques propositions avec des courbes elliptiques

Perspectives

- Quelques ccTLD (.se, .br, ..., *pas* .fr)
- .org
- .gov par décision du GAO
- Consultation pour la signature de “.”
- Trust Anchor Repositories (exemple : ITAR)
- DLV RR
- Dernières nouvelles : *root signed by year’s end*

Questions ?

Références

- RFC 403[345], 4431 (DLV), 4641 (operations), 5155 (NSEC3)
- http://www.dnssec.net/
- http://www.dnssec-deployment.org/
- http://dnsseccoalition.org/
- http://www.dnssec-tools.org/
- http://www.hznet.de/dns/zkt/
- http://www.unixwiz.net/techtips/iguide-kaminsky-dns-vuln.html

Rappels(packet)

- Header,
  Question, Answer, Authority, Additional
- QID (16 bits), Opcode, Rcode, flags and section RR counts

Rappels(flags)

- QR (query or response)
- AA (authoritative answer) (response)
- TC (truncation)
- RD (recursion desired) (query/copied)
- RA (recursion available) (response)
- AD (authentic data) (response)
- CD (checking disabled) (query/copied)
- DO (DNSSEC OK) (EDNS0) (query/copied)

Rappels(rcodes)

- NOERROR
- FORMERR
- SERVFAIL
- NXDOMAIN
- NOIMP
- REFUSED
- YXDOMAIN, YXRRSET, NXRRSET, NOTAUTH, NOTZONE (dynamic updates)

Rappels(EDNS0)

- Pseudo-RR OPT
- Version (0), extended-rcode, UDP payload size (maximum, default 512), DO bit, AVPs

Kaminsky(1)

- Attaque contre les serveurs caches (et aussi mais sans intérêt les resolvers)
- Requêtes depuis des clients sous contrôle
- Réponses forgées depuis l'Internet avec une réponse correcte et des sections plausibles (passe le "in bailiwick") mais empoisonnées
- Recherche une collision sur les adresses, ports et le query/transaction ID sur 16 bits...

Kaminsky(2)

- Réponse 1 : “ingress filtering” (BCP 38 et 84) contre les fausses adresses sources
- Réponse 2 : randomiser le port source pour ajouter un peu d’entropie
- Réponse 3 : passer à TCP, QID plus long, bit de casse, etc (mais il est déjà trop tard)
- Réponse 4 : DNSSEC

National Telecommunications and Information Administration

About NTIA

Issues

NTIA Offices
- **Asst. Secretary**
- **Domestic Policy**
- **International**
- **Spectrum**
- **Telecom Research**
- **Grants**

Public Notices

Publications & Reports

Media & Press

Speeches

NTIA Jobs

Dept. of Commerce

Commerce Department to Work with ICANN and VeriSign to Enhance the Security and Stability of the Internet's Domain Name and Addressing System

For Immediate Release: June 3, 2009
NTIA Contact: Bart Forbes, (202) 482-7002 or press@ntia.doc.gov
NIST Contact: Chad Boutin, (301) 975-4261 or boutin@nist.gov

WASHINGTON — The U.S. Department of Commerce's National Telecommunications and Information Administration (NTIA) and National Institute of Standards and Technology (NIST) announced today that the two agencies are working with the Internet Corporation for Assigned Names and Numbers (ICANN) and VeriSign on an initiative to enhance the security and stability of the Internet. The parties are working on an interim approach to deployment, by year's end, of a security technology -- Domain Name System Security Extensions (DNSSEC) -- at the authoritative root zone (i.e., the address book) of the Internet. There will be further consultations with the Internet technical community as the testing and implementation plans are developed.

The Domain Name and Addressing System (DNS) is a critical component of the Internet infrastructure. The DNS associates user-friendly domain names (e.g., www.commerce.gov) with the numeric network addresses (e.g., 170.110.225.163) required to deliver information on the Internet, making the Internet easier for the public to navigate. The accuracy, integrity, and availability of the

SEARCH: Go

American Recovery and Reinvestment Act

For NTIA's efforts, visit **NTIA: Recovery Act**.

Broadband Technology Opportunities Program