Sector 2007, Toronto, Canada

DNSSEC: Theory and Worldwide Operational Experiences

Paul Wouters
paul@xelerance.com

November 20, 2007

Who are we?

Xelerence Corporation is a company with a dedicated team of experienced software developers, network designers and consultants providing support, development and network design services for businesses from ISP's to Fortune 100 companies

Our initial flagship solution “Openswan” is found as the core of many IPsec based VPN products, ranging from enterprise rollouts to consumer electronics.

BIAS (Dis)claimer

xelerance™

Xelerence Corporation is heavilly involved in the IETF and RIPE communities with the design, development and implementation of the DNSSEC standards, software, and hardware appliances.

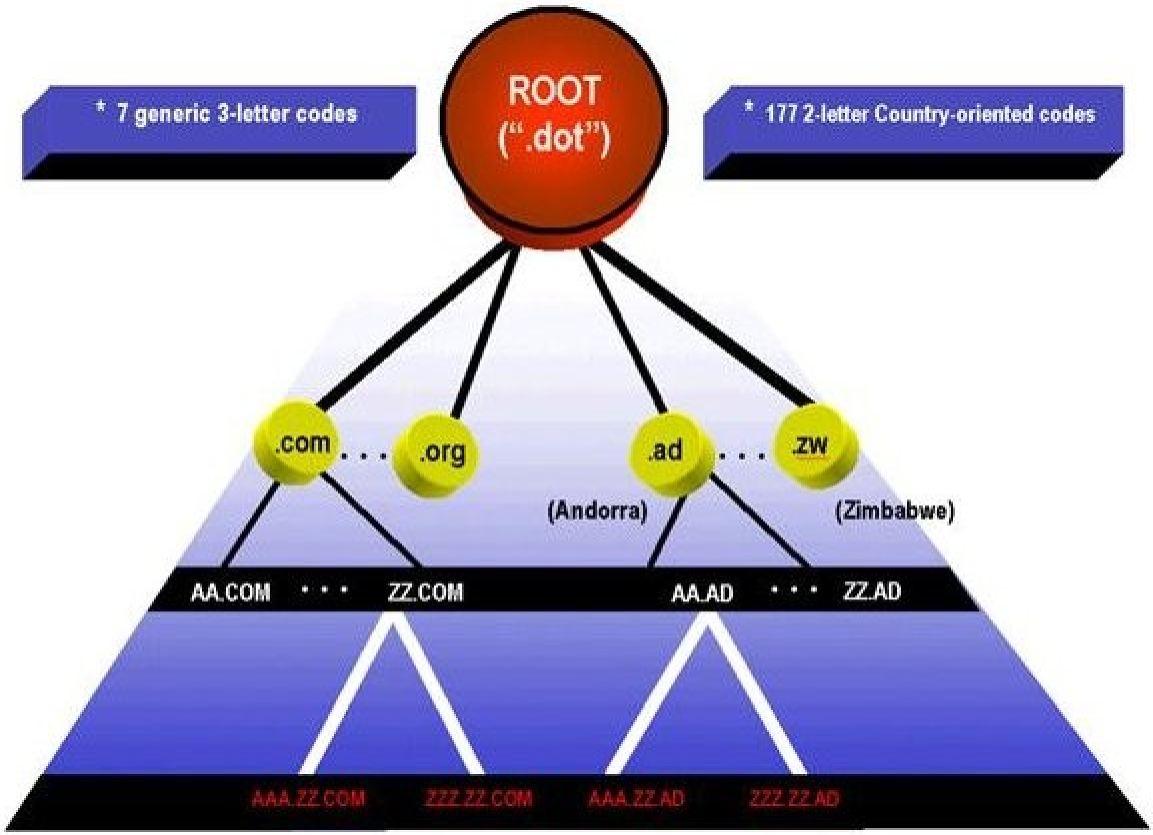
The Domain Name System (DNS)

The DNS translates domain names to IP addresses and back via a distributed method. It also lists Mail eXchange (MX) records et. al.

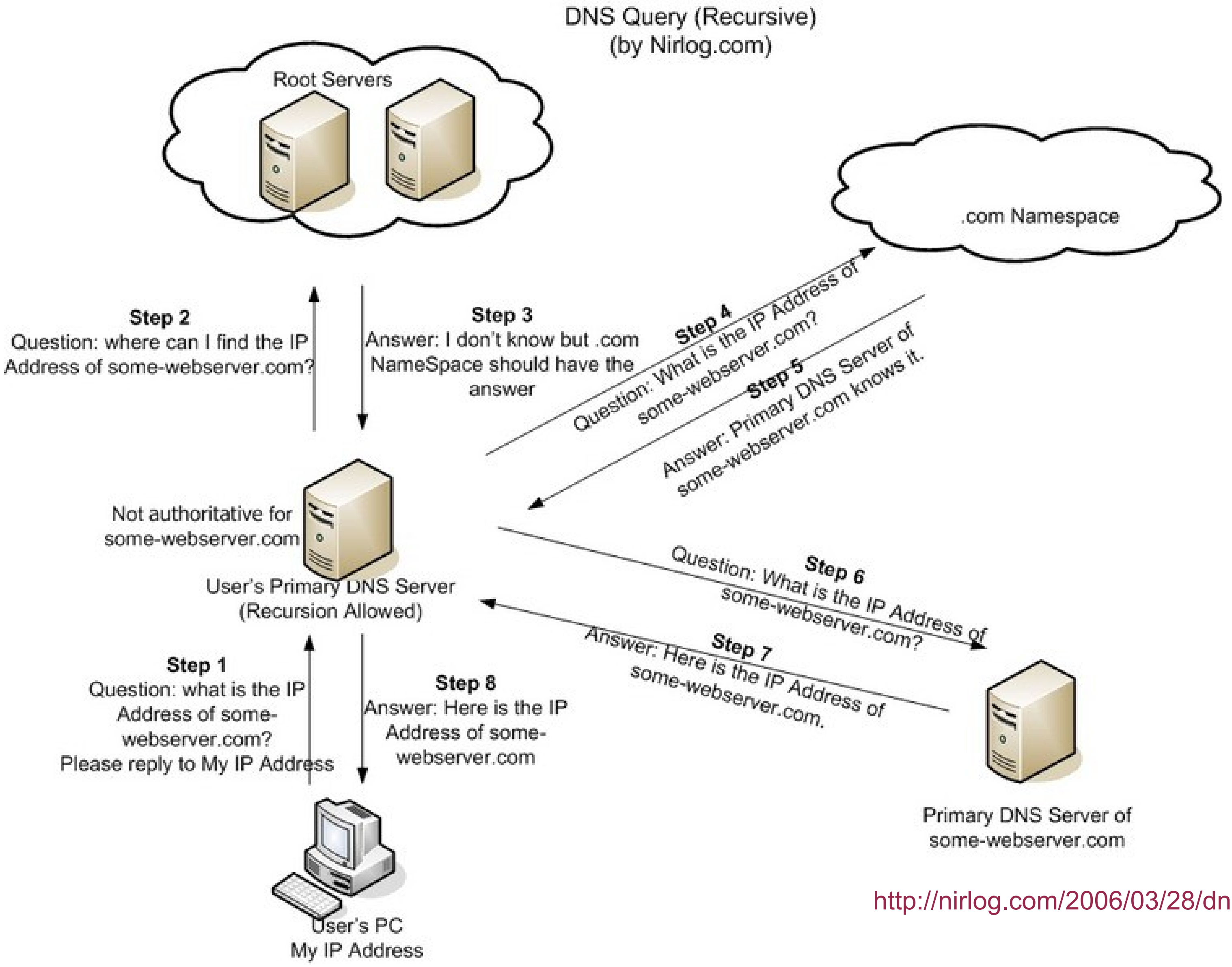
In recent years, people have put all kind of important information in the DNS, with the assumption that it is “safe” or even “private”, such as LDAP / Active Directory, SPF, NAPTR/SRV for SIP, ENUM, public keys, fingerprints..

DNS is hierachical and distributed

What is DNS? An arbitrary, hierarchical naming convention, primarily based on geographical designations.



Basic Architecture of DNS



DNS Query (Recursive)
(by Nirlog.com)

Root Servers

.com Namespace

Step 2
Question: where can I find the IP Address of some-webserver.com?

Step 3
Answer: I don't know but .com NameSpace should have the answer

Step 4
Question: What is the IP Address of some-webserver.com?

Step 5
Answer: Primary DNS Server of some-webserver.com knows it.

Not authoritative for some-webserver.com

User's Primary DNS Server
(Recursion Allowed)

Step 6
Question: What is the IP Address of some-webserver.com?

Step 7
Answer: Here is the IP Address of some-webserver.com.

Step 1
Question: what is the IP Address of some-webserver.com?
Please reply to My IP Address

Step 8
Answer: Here is the IP Address of some-webserver.com

Primary DNS Server of some-webserver.com

User's PC
My IP Address

http://nirlog.com/2006/03/28/dns-amplification-attack/

15 attacks on DNS

It takes a lot of queries to get an answer

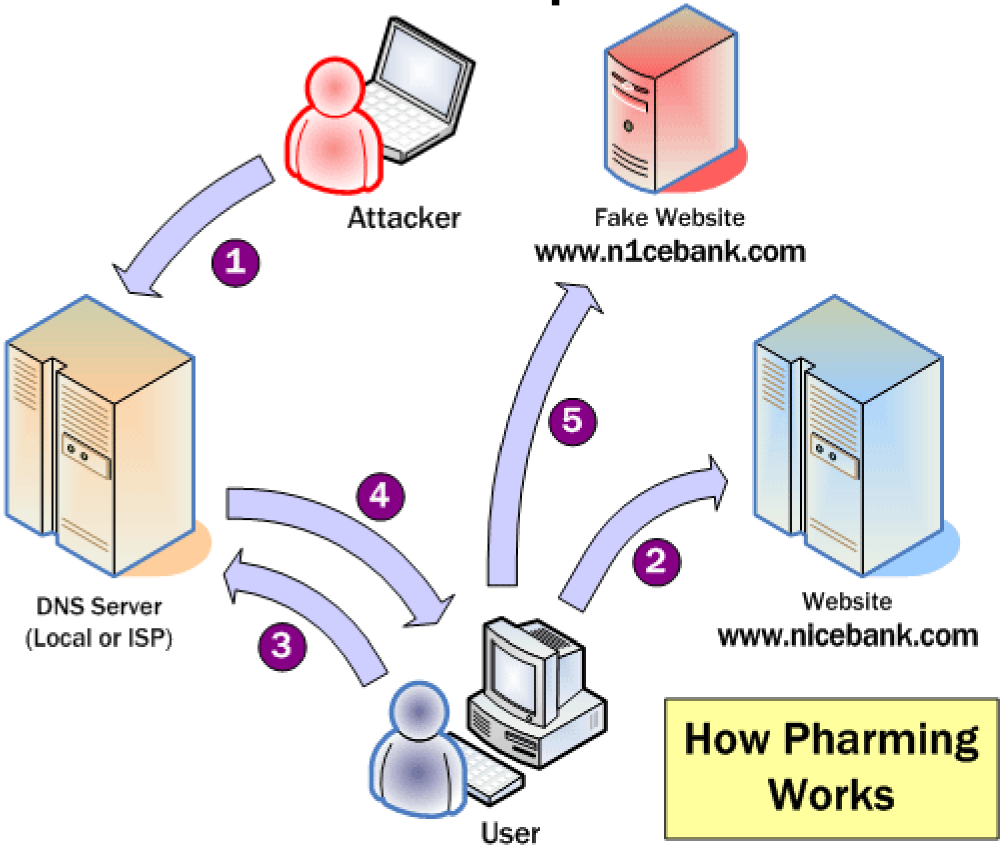
[let me show you....]

Attack 1
Endpoint DNS spoofing

(C)opyright http://www.flickr.com/photos/hsaito/111233121/

Attack 2
ISP cache poisoning, then spam

In 2006 Rogers and Bell Canada got their nameservers poisoned with TD Canada Trust and CIBC domains.



How Pharming Works

Localised attack by remote attacker

http://palisade.plynt.com/issues/2006Mar/pharming/

Attack 3
BIND vulnerability: Predict ID's

Attacker queries target DNS to obtain the random ID
Attacker predicts the next (not really random) ID used

Attacker asks for www.spoofed.com, triggering DNS server to go find the answer.

Attacker “answers” on behalve of www.spoofed.com's nameserver. Required about 30 packets to get the right “random” ID.

DNS server now has a false answer cached, which it will hand out to other clients asking for www.spoofed.com

Attack 4
Sysadmin typo abuse

http://www.julianhaight.com/msnhack.html

Before September 6, 2007:

```
$ dig msn.com.tw @d.twnic.net.tw.

;; AUTHORITY SECTION:
msn.com.tw.         86400   IN      NS      dns1.cp.msft.net.
msn.com.tw.         86400   IN      NS      dns1.dc.msft.net.
msn.com.tw.         86400   IN      NS      dns1.tk.msft.net.
msn.com.tw.         86400   IN      NS      dns3.uk.msft.net.
msn.com.tw.         86400   IN      NS      dns.cpmsft.net.
```

Attack 4
Sysadmin typo abuse

http://www.julianhaight.com/msnhack.html

Before September 6, 2007:

```
$ dig msn.com.tw @d.twnic.net.tw.

;; AUTHORITY SECTION:
msn.com.tw.        86400   IN     NS     dns1.cp.msft.net.
msn.com.tw.        86400   IN     NS     dns1.dc.msft.net.
msn.com.tw.        86400   IN     NS     dns1.tk.msft.net.
msn.com.tw.        86400   IN     NS     dns3.uk.msft.net.
msn.com.tw.        86400   IN     NS     dns.cpmsft.net.
```

Attack 5
NXDOMAIN “helpers”

OpenDNS service

(people have to configure this themselves)

goggle.com -> google.com

But what if goggle.com is a “real” domain?

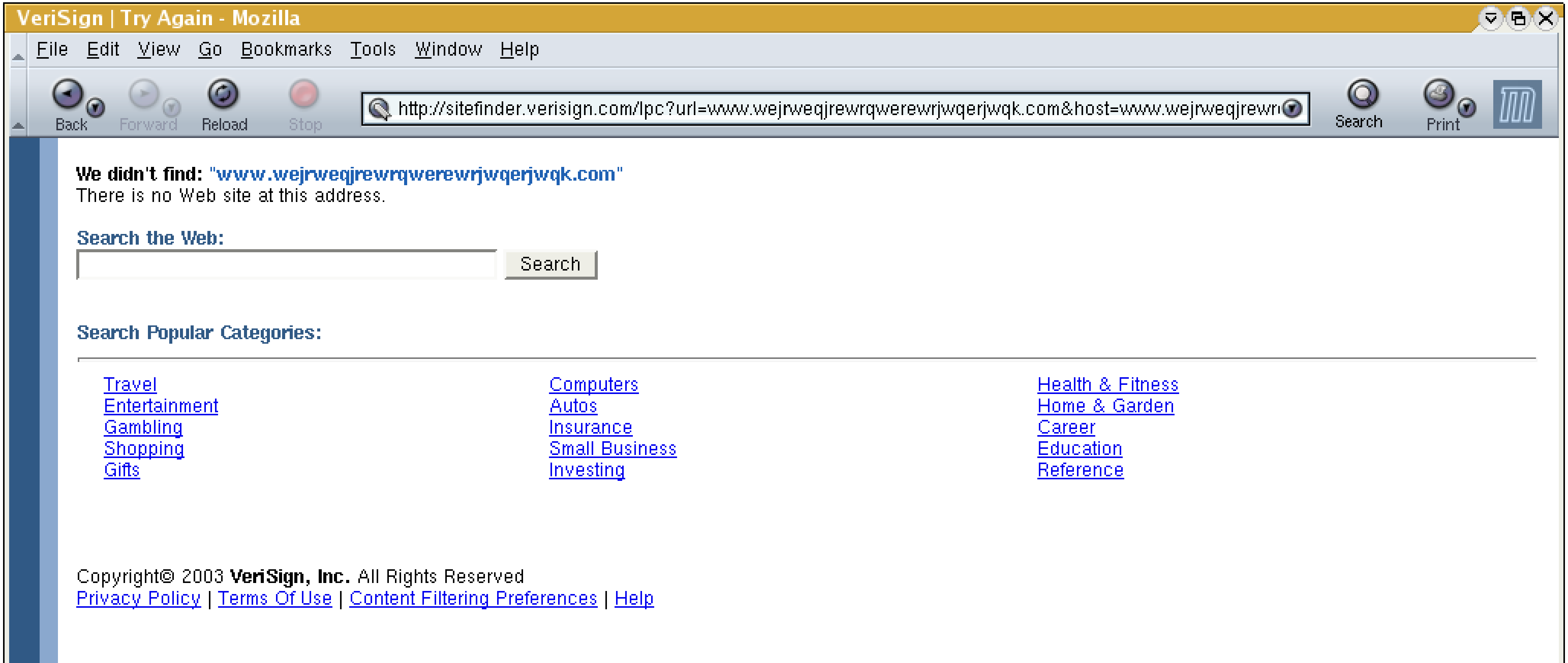
But what if OpenDNS does not like domain X?

Attack 6
NXDOMAIN thieves [part 1]

ISP's abusing nameservers assigned to users via DHCP

Attack 7
NXDOMAIN thieves [part 3]

It's a bit worse when Versign, the guardian for .com does it – and with a MX wildcard!


VeriSign | Try Again - Mozilla
File Edit View Go Bookmarks Tools Window Help
Back
Forward
Reload
Stop
Search
Print

http://sitefinder.verisign.com/lpc?url=www.wejrweqjrewrqwerewrjwqerjwqk.com&host=www.wejrweqjrewr

We didn't find: "www.wejrweqjrewrqwerewrjwqerjwqk.com"
There is no Web site at this address.

Search the Web:

Search

Search Popular Categories:

Travel
Entertainment
Gambling
Shopping
Gifts

Computers
Autos
Insurance
Small Business
Investing

Health & Fitness
Home & Garden
Career
Education
Reference

Copyright© 2003 **VeriSign, Inc.** All Rights Reserved
Privacy Policy | Terms Of Use | Content Filtering Preferences | Help

Attack 8
The government knows best:

An increase in government ordered DNS meddling

No YouTube in Thailand over insulted the king [mar 2007]

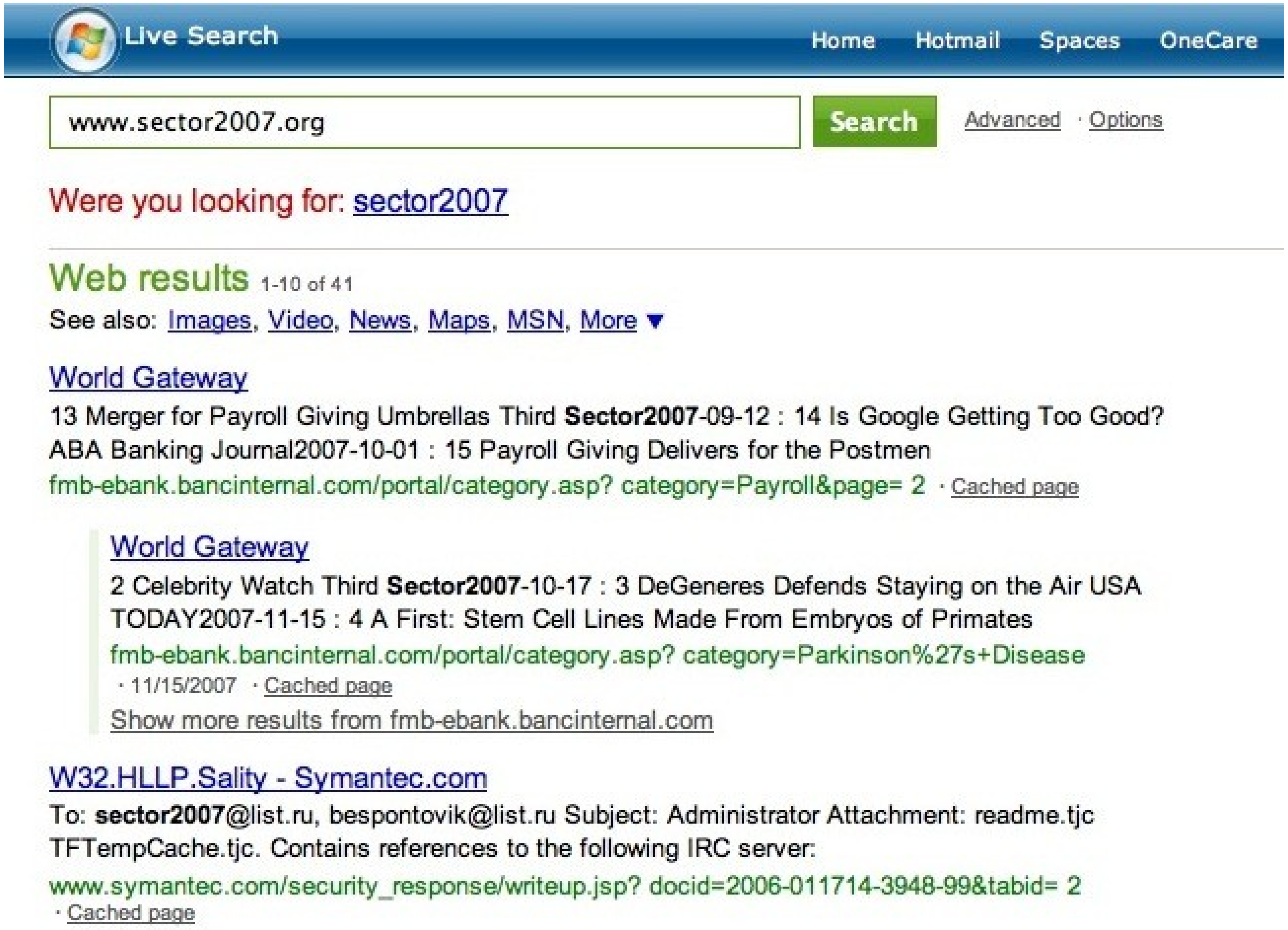
No Youtube in Turkey over insulting nation [sep 2007]

ISPs are forced to ban hate sites (eg France, Germany)

FBI et all redirecting traffic with a 'Moral and Ethics' page

Attack 9
The NXDOMAIN vendor thieves..

Everyone wants to h$lp you



www.sector2007.org

Were you looking for: sector2007

Web results 1-10 of 41

See also: Images, Video, News, Maps, MSN, More ▼

World Gateway
13 Merger for Payroll Giving Umbrellas Third **Sector2007**-09-12 : 14 Is Google Getting Too Good? ABA Banking Journal2007-10-01 : 15 Payroll Giving Delivers for the Postmen
fmb-ebank.bancinternal.com/portal/category.asp? category=Payroll&page= 2 · Cached page

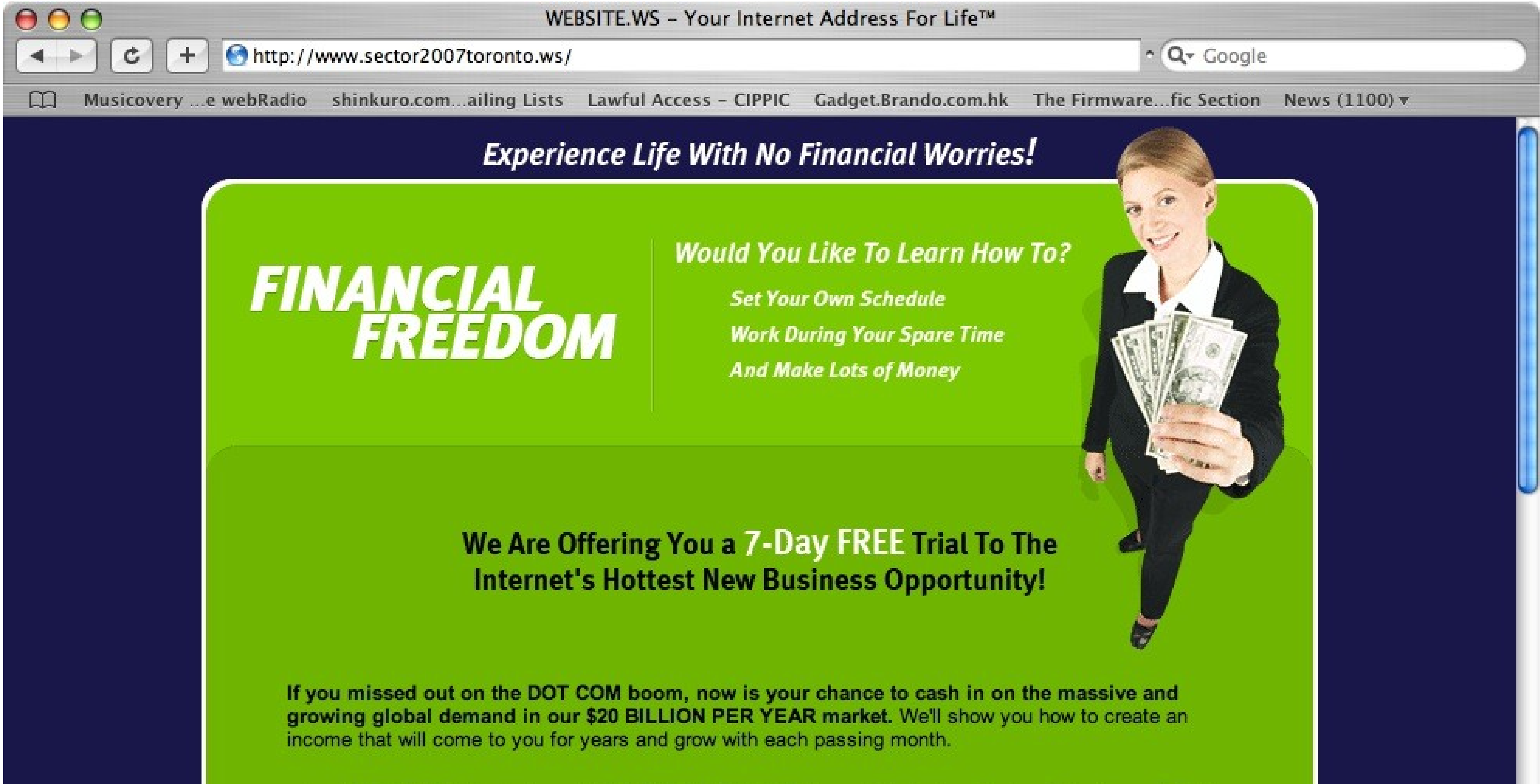
World Gateway
2 Celebrity Watch Third **Sector2007**-10-17 : 3 DeGeneres Defends Staying on the Air USA TODAY2007-11-15 : 4 A First: Stem Cell Lines Made From Embryos of Primates
fmb-ebank.bancinternal.com/portal/category.asp? category=Parkinson%27s+Disease
· 11/15/2007 · Cached page
Show more results from fmb-ebank.bancinternal.com

W32.HLLP.Sality - Symantec.com
To: **sector2007**@list.ru, bespontovik@list.ru Subject: Administrator Attachment: readme.tjc TFTempCache.tjc. Contains references to the following IRC server:
www.symantec.com/security_response/writeup.jsp? docid=2006-011714-3948-99&tabid= 2
· Cached page

Security Education Conference

Attack 10
NXDOMAIN thieves [part 2]

Some TLD's want to to scam you....



WEBSITE.WS – Your Internet Address For Life™

http://www.sector2007toronto.ws/

Experience Life With No Financial Worries!

FINANCIAL FREEDOM

Would You Like To Learn How To?

Set Your Own Schedule

Work During Your Spare Time

And Make Lots of Money

We Are Offering You a 7-Day FREE Trial To The Internet's Hottest New Business Opportunity!

If you missed out on the DOT COM boom, now is your chance to cash in on the massive and growing global demand in our $20 BILLION PER YEAR market. We'll show you how to create an income that will come to you for years and grow with each passing month.

Attack 11
Nationwide DNS spoofing China

Some TLD's want to protect you....
(September 2002)

If there is “minghui” anywhere in the URL string, the DNS server will return the fake ip address 64.33.88.161

minghui.org is the website of Falun Gong

Attack 12
Resolver games: Wildcard record

*.com.boldlygoingnowhere.org

Combined with malware setting your DNS search suffix to:

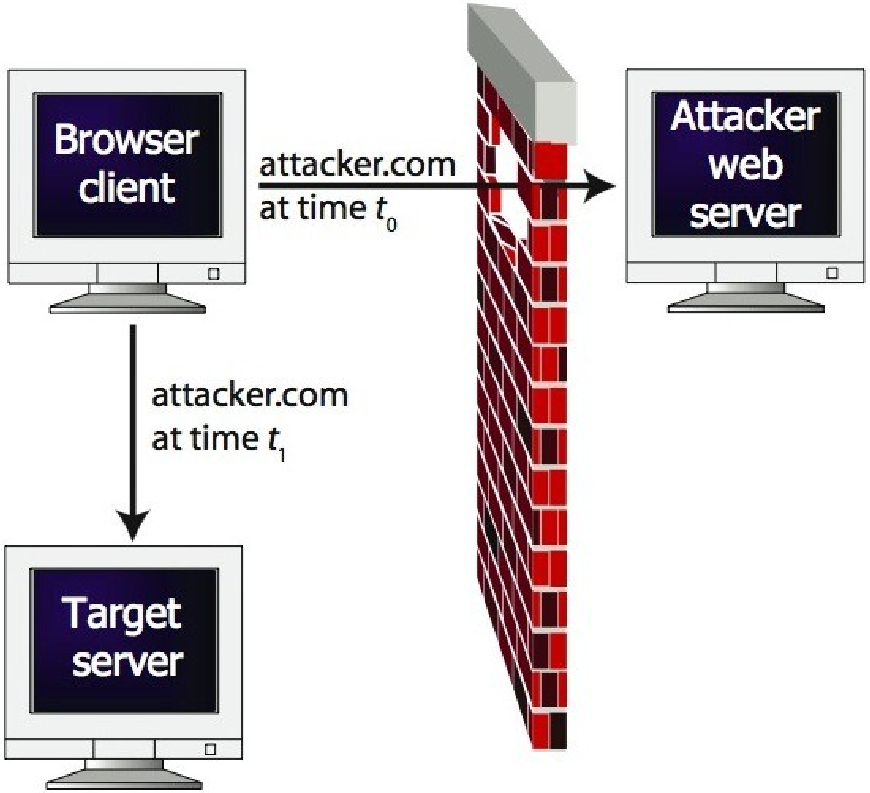
“com.boldlygoingnowhere.org”

Will change your query for **www.google.com** to

www.google.com.com.boldlygoingnowhere.org

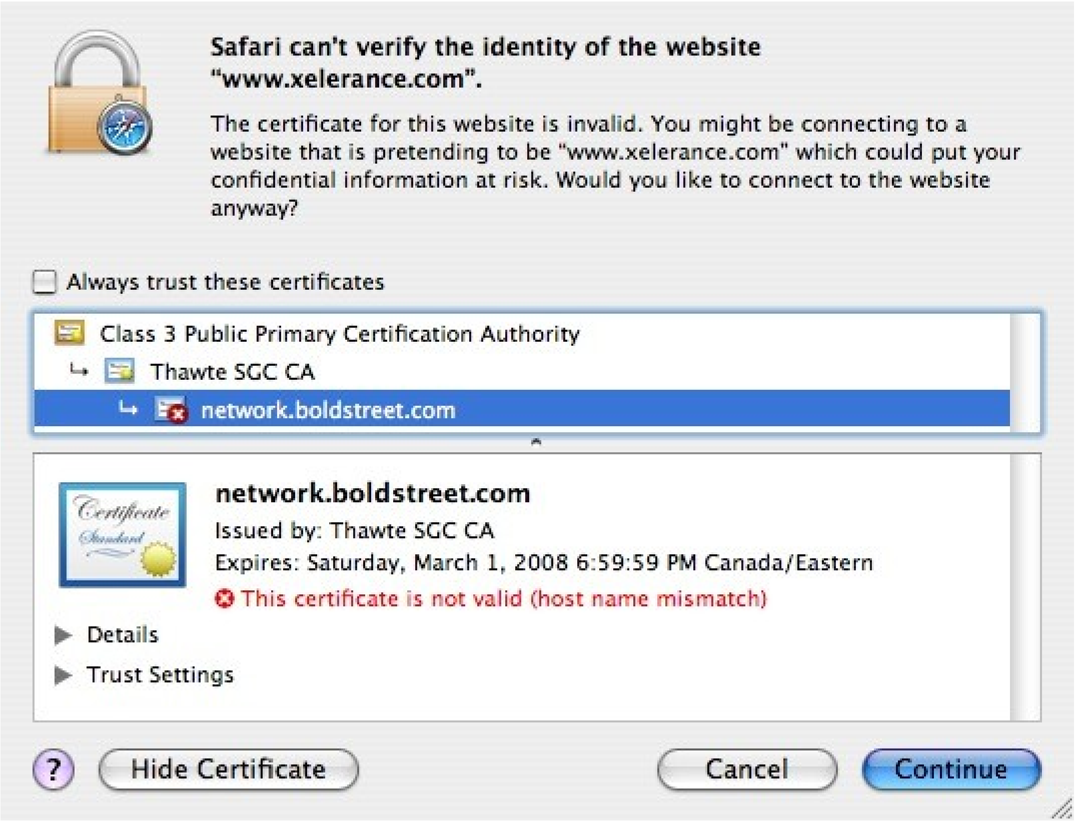
(Microsoft not affected, they hardcode some *.microsoft.com in the resolver code)

Attack 13
DNS rebinding



Demo site:
http://www.jumperz.net

Attack 14
Captive Portals



Safari can't verify the identity of the website "www.xelerance.com".

The certificate for this website is invalid. You might be connecting to a website that is pretending to be "www.xelerance.com" which could put your confidential information at risk. Would you like to connect to the website anyway?

□ Always trust these certificates

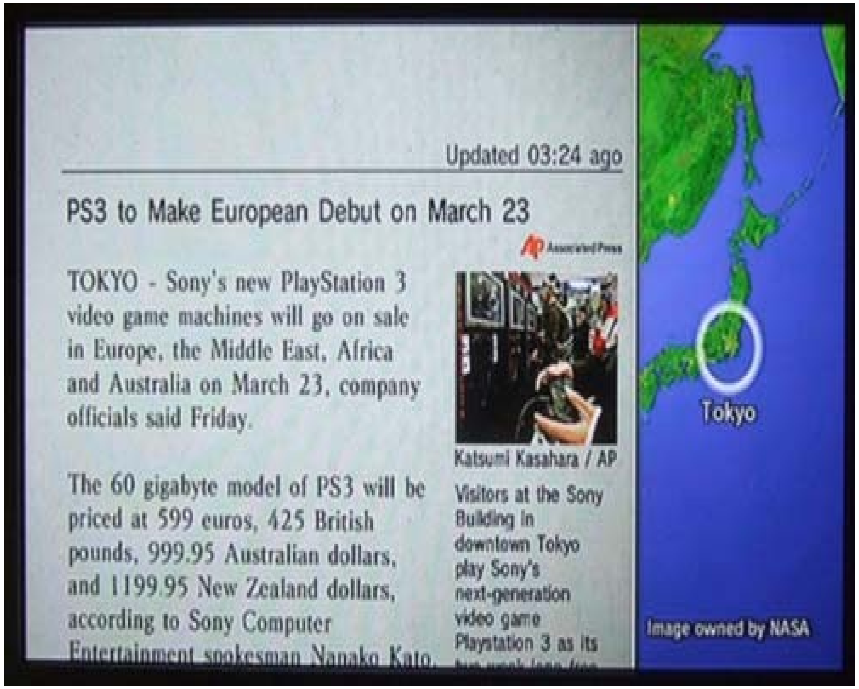
Class 3 Public Primary Certification Authority
↳ Thawte SGC CA
↳ network.boldstreet.com

network.boldstreet.com
Issued by: Thawte SGC CA
Expires: Saturday, March 1, 2008 6:59:59 PM Canada/Eastern
This certificate is not valid (host name mismatch)

xelerance

Attack 15
Run your own (fake) AUTH server

I want to add my own RSS feeds to the Wii News menu. So I hijacked their DNS to send it to through my own servers and see what I could run against it as exploit.



Updated 03:24 ago

PS3 to Make European Debut on March 23

AP Associated Press

TOKYO - Sony's new PlayStation 3 video game machines will go on sale in Europe, the Middle East, Africa and Australia on March 23, company officials said Friday.

The 60 gigabyte model of PS3 will be priced at 599 euros, 425 British pounds, 999.95 Australian dollars, and 1199.95 New Zealand dollars, according to Sony Computer Entertainment spokesman Nanako Kato.

Katsumi Kasahara / AP

Visitors at the Sony Building in downtown Tokyo play Sony's next-generation video game Playstation 3 as its

Tokyo

Image owned by NASA

SECTOR
Security Education Conference

Everybody wants your DNS

Internet Service Providers
Wifi hotspots / captive portals
Applications
Websites (activeX, java, javascript, flash)
Operating Systems
cc:TLD's

oh, and hackers, spammers, phishers, pharmers

See also: “**DNS Trheat Analyses**” by Santcroos, Kolkman

http://nlnetlabs.nl/downloads/se-consult.pdf

What is DNSSEC?

DNSSEC is a protocol that secures the DNS against spoofing and hijacking attacks

DNSSEC is a cryptographically protected DNS

DNSSEC builds a path of trust from a parent zone to a child zone to a grand child zone [...]

DNSSEC allows multiple “Secure Entry Points”

What is DNSSEC not

It's not about encrypting the DNS or privacy of DNS data

It's not about X.509, SSL certificates, or Central Authorities

It's not about making a secure storage point for others
(according to the designers of DNSSEC, not its users)

History of DNS(SEC)

(see http://nlnetlabs.nl/dnssec/history.html)

1983: Mockapetris invents DNS
1986: IETF RFC1034 and 1035
1988: Widespread use
1990 Steve Bellovin discovers flaws inDNS. Is kept secret
1995 Flaw is published, IETF starts to talk about DNSSEC
1997 RFC2065 – first attempt at DNSSEC
1999 RFC2535 – DNSSEC looks finished, but a lot of discussion on parent-child interaction/authority
2000 First DNSSEC TLD tested, .nl.nl shadow zone
2001 SECREG.nl experiment – though successful, .nl does not continue (http://www.xtdnet.nl/paul/dnssec/
2001 NLnetlabs becomes a major developer with the NSD nameserver supporting DNSSEC and the LDNS DNSSEC library.

History of DNS(SEC)

(see http://nlnetlabs.nl/dnssec/history.html)

2002/2003 RFC2535bis – the DS record introduced
2003 Dutch ISP xtdnet.nl enables DNSSEC on all customer domains
2005 RFC4033, 4034 and 4035 published – "DNSSEC"
2005 Sweden becomes first TLD to use DNSSEC
2006 RIPE enables DNSSEC for their in-addr.arpa.
2007 Deployment worldwide increased to 5 TLD's
2007 Zone walking is still discussed. The solution of the NSEC3 record is still being discussed.
2007 OPT-IN in still being discussed to reduce memory requirements in large zones files.
2007 The larger TLD's are still working on faster hardware and protocol tweaks to be able to sign their zones daily (or in some cases hourly)

DNSSEC requirement: EDNS0

A method for adding more flags and options to the DNS.

DNS packets we not larget then 512 bytes, but DNS packets with EDNS0 can be larger then 512 bytes

Defined in RFC2671 – published in 1999

Still a lot of firewalls and/or consumer products do not properly handle or relay EDNS0

This is a deployment concern for resolvers

client-resolver-auth server

Client – Resolver communication is assumed to be trusted. If not, you can:

- Run resolver on the client itself (recommended)
- Setup trusted connection to resolver (TSIG or VPN)

Client can ask “do DNSSEC for me” with the DO bit
Client can just ask for DNS and trust the AD bit

With ISP's using DNSSEC enabled nameservers, the biggest DNS spoofing/hijacking attacks would be twarted. ISP's DNSSEC enabled nameservers don't help you when you are on an insecure wifi network.

DNSSEC components

DNSSEC signers: Generate cryptographic key pairs and signing zone files

AUTHORITATIVE Namservers: Publishing DNSSEC zonefiles. Performs no crypto operations – just serves

Recursive Resolving Nameservers: Querying DNSSEC records and cryptographically verifying the records are genuine. May or may not use crypto

Application Interface: Enhance applications to give proper feedback to the user (not just ServFail or 'not found')

DNSSEC signers

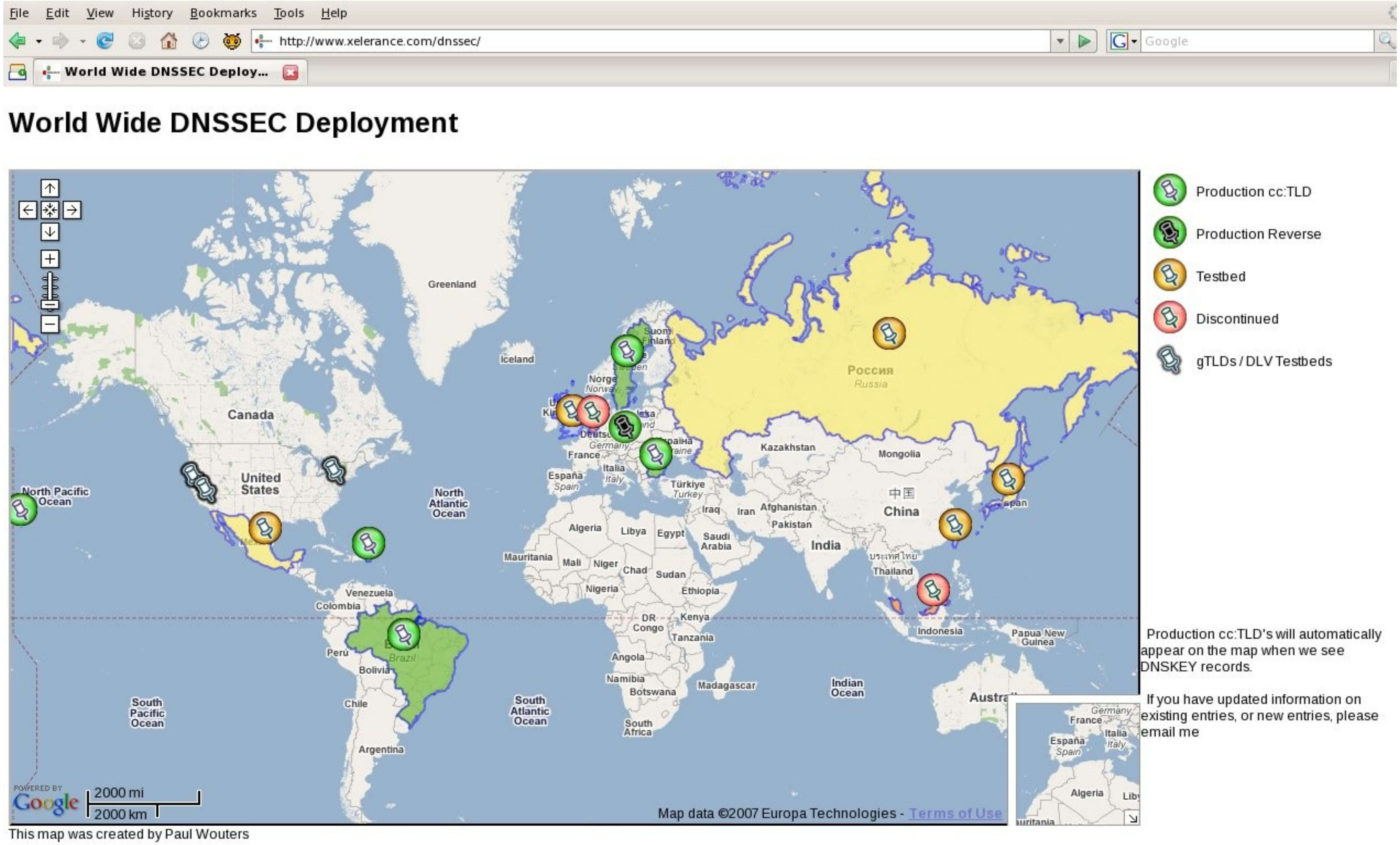
BIND, www.isc.org, Internet Software Consortium (using OpenSSL)

Donuts, dnssec-tools.org, SPARTA Inc (wrapper around BIND)

Maintkeydb, www.ripe.net/disi, RIPE (wrapper around BIND)

Crypto is hard – be careful to trust others

Current DNSSEC TLD deployment



World Wide DNSSEC Deployment

- Production cc:TLD
- Production Reverse
- Testbed
- Discontinued
- gTLDs / DLV Testbeds

Production cc:TLD's will automatically appear on the map when we see DNSKEY records.

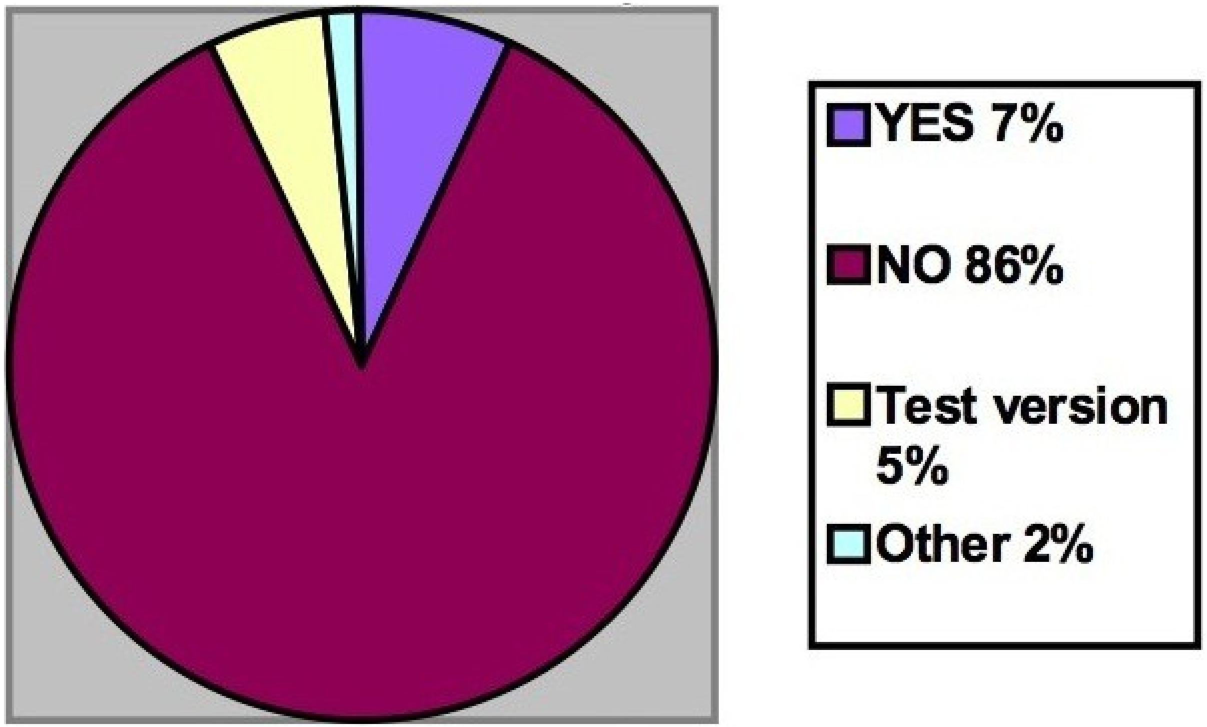
If you have updated information on existing entries, or new entries, please email me

This map was created by Paul Wouters

DNSSEC survey by ccNSO Council

October 27 2007 65 ccTLD's responded

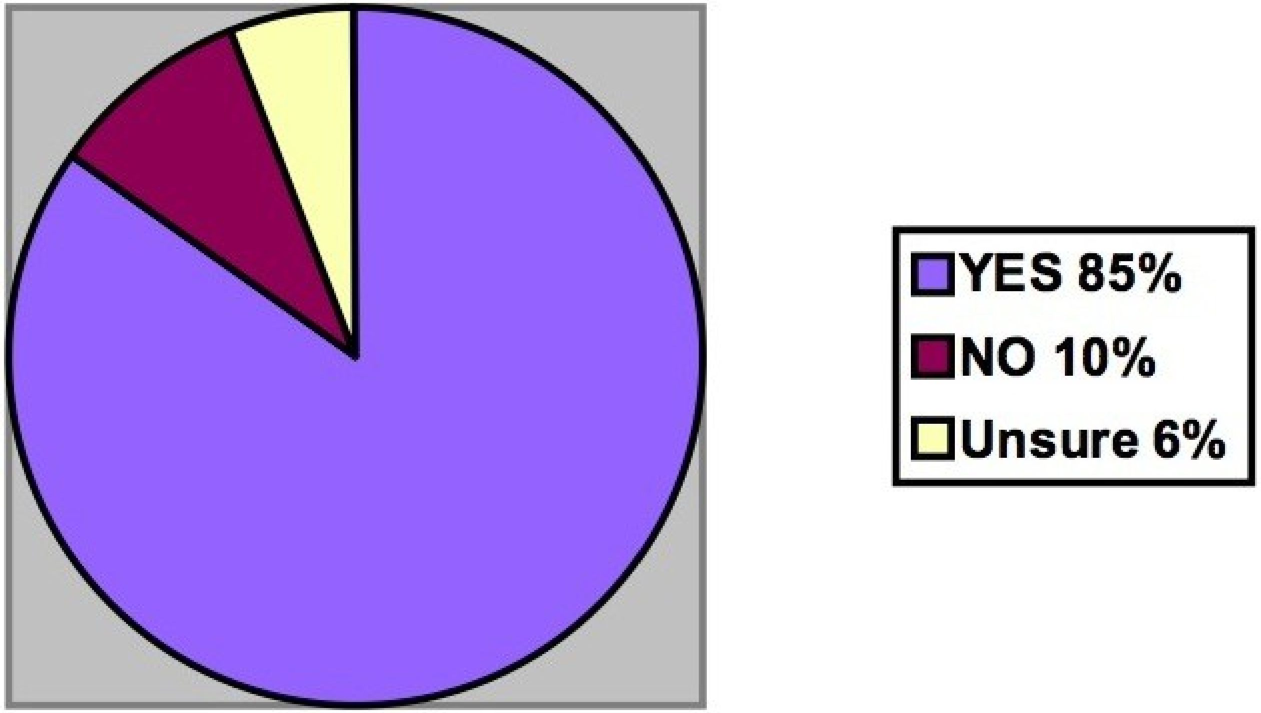
Have you implemented DNSSEC?



DNSSEC survey by ccNSO Council

October 27 2007 65 ccTLD's responded

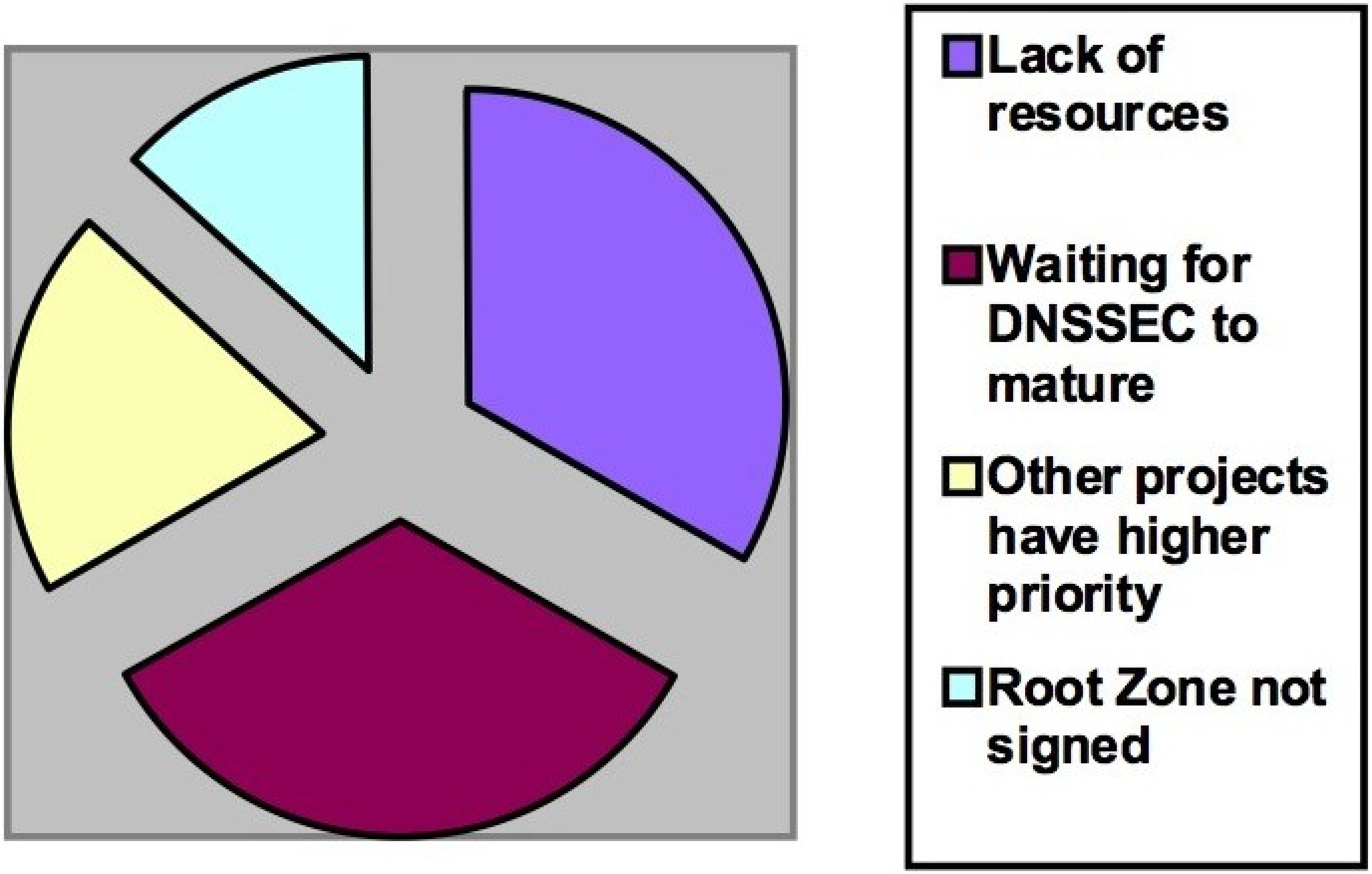
If you have not implemented DNSSEC, are you planning to implement it?



DNSSEC survey by ccNSO Council

October 27 2007 65 ccTLD's responded

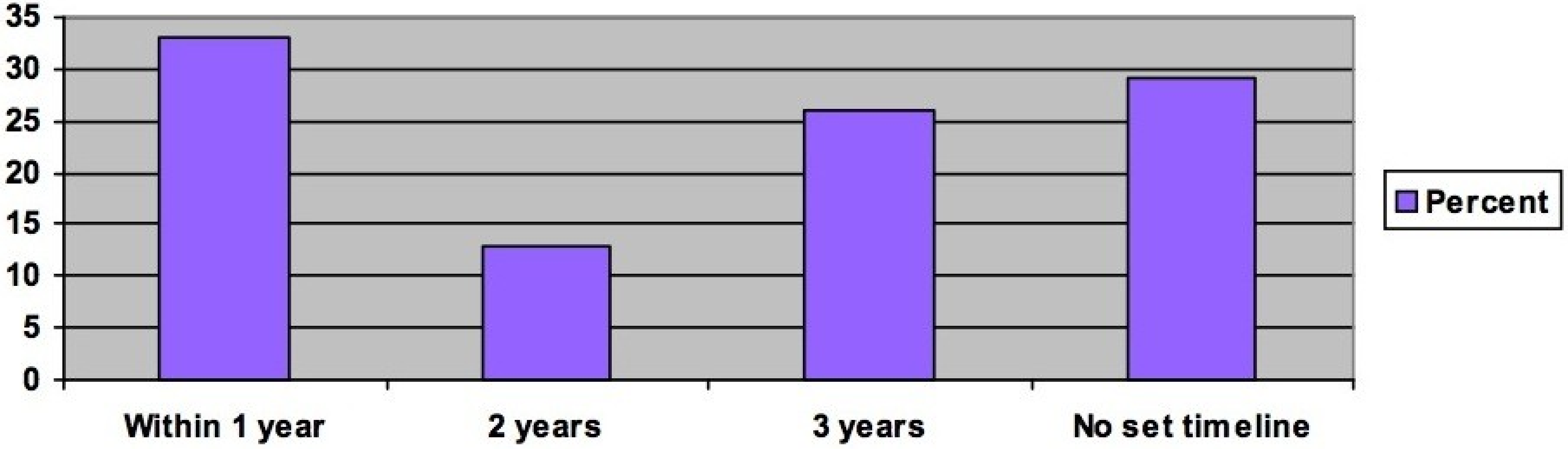
If you have not implemented DNSSEC,What are the reasons for not implementing DNSSEC?



DNSSEC survey by ccNSO Council

October 27 2007 65 ccTLD's responded

If you have not implemented DNSSEC, When are you planning to implement DNSSEC?



Resolver Deployments

21 september 2007 – first large ISP deployment of DNSSEC enabled resolver in Sweden.

Instantly broke connectivity for many people. It was disabled the same day.

In the following weeks it became clear that many cheap consumer routers, do not handle the AD bit correctly, and dropped the DNS packets. Partial work around added to BIND.

Broken routers were found for D-LINK, Netgear, Gigabyte, and Zyxel.

Application support in a very premature state

- Nameservers support DNSSEC
  - nsd – authoritative only, signing tools seperate
  - bind – fully implemented (invluding DLV)
- Various testing tools written
  - dnssec-tools.org – management tools, validation tools
  - www.ripe.net/disi/ – management tools
  - www.nlnetlans.nl/ldns/ - validation tools, firefox plugin
- Various application modifications to support DNSSEC
  - Postfix, Sendmail, Openswan, Firefox patches by dnssec-tools.org
- Stubs and beginnings of low level support
  - openSSH (SSH implementation)
  - Openswan (IPsec implementation)
  - GLIBC (posix implementation)

How does DNSSEC work?

New DNSSEC record types

DNSKEY record - Public key of keypair that signs DNS data in the zone. Usually two or three keys present due to the complexity of “Key Rollover”. These keys are called the Zone Signing Key and Key Signing Key.
RRSIG record - The actual digital signature over an RRset of DNS data - made by a DNSKEY's private key.
NSEC/NSEC3 record - Pointer to next DNS record. Used for “authenticated denial of existance” of a DNS query.

DS record - Delegated Signer. Hash of the key of a DNSSEC secured child zone. Used to build chains of trust. (similar to “glue” records, but authoritative/signed)

The DNSKEY record

```
xelerance.com.    3600 IN DNSKEY 256 3 5 (

AwEAAamc7W2EQdv34ZyUFapilEzOmcxZE
8YQvJ3o1L+QdWU0O7VspH5iNXE16bWrez
7tOHBPZfxsJYurF0GQMXQ+kVh0Ls0uPyhv
QkE+arcQhXG2scCDPIBmD0iuVx50+qBN9
0QnXmESoywVSPJmA11HAPrAC5ncM2o7y
CrOsQ7ej

) ; key id = 18603
```

The RRSIG record

```
www.xelerance.com.    3600   IN A 193.110.157.129

www.xelerance.com.    3600   IN RRSIG A 5 3 3600
  20071214195937   (    20071114195937 18603
  xelerance.com.
  SH/yeUTkoD1x6W1oHa Kn1O57ZUVsShY
  vgDPy26pFhztdEc9hXiXSVX15Hh4jlxEJNr
  M8A61HZftIV3ujr8CwfPLf3BD6nJVjEt+Xxs
  FxWFOd01co04WzFFhuluhCq5z0vHJXOX
  oZjU= )
```

The DS record

```
xelerance.se.    43200    IN    DS    14850 5 1 (
  B8D93CB3FF749812D5FECD38967F525BF
  D53DFED )
```

This record (in the zone .se) is signed by the “.se” DNSKEY. The value is the hash of the DNSKEY of “xelerance.se”

How to sign non-existent answers?

How do you convey that “non-existent.example.com” does not exist:

Without making an infite list of possible hostnames

Without requiring custom signed answers (too cpu intensive and requires private key on nameserver)

Supporting wild card records

Using some kind of DNS record that can be signed with an RRSIG

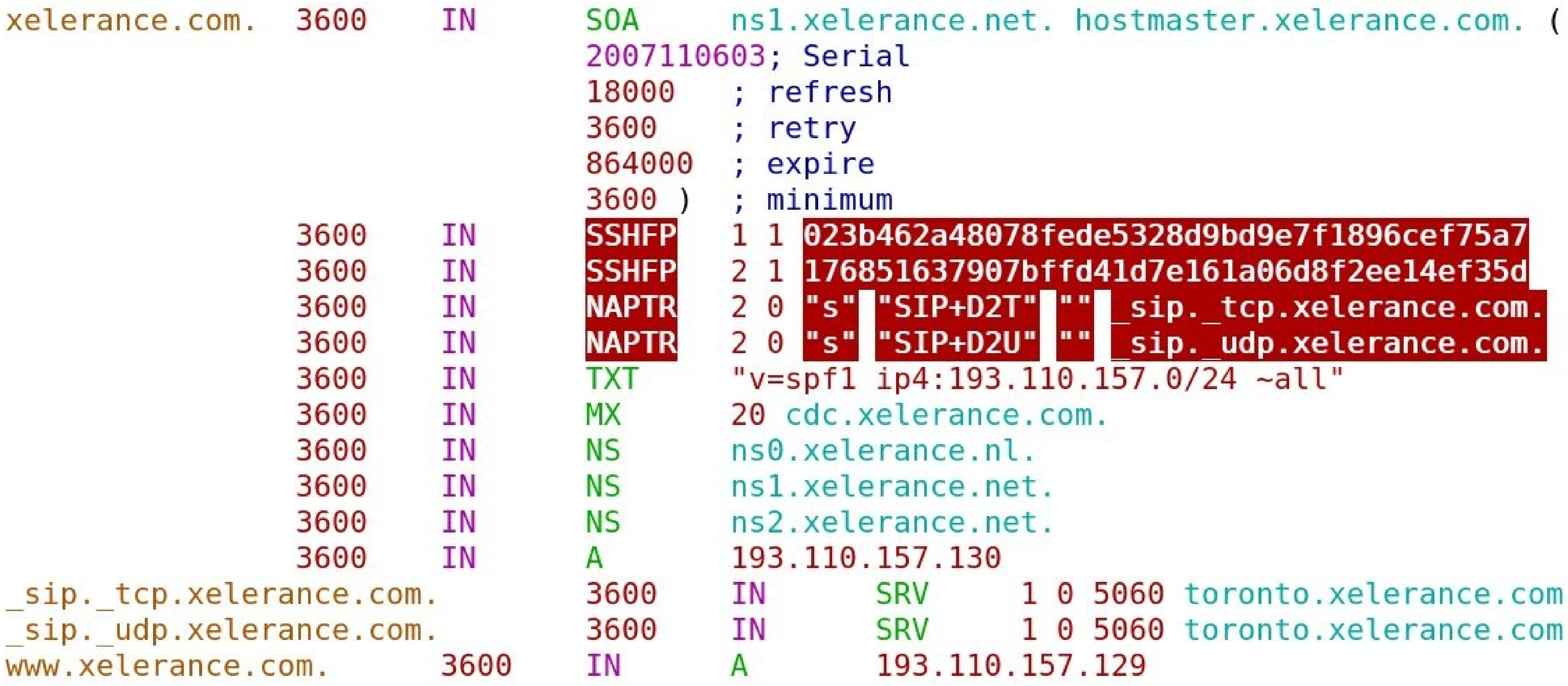
The NSEC record

```
rcmp.xelerance.com. 3600 IN NSEC
          secure.xelerance.com. A RRSIG NSEC
```

We know that alphabetically, there is nothing between “rcmp.xelerance.com” and “secure.xelerance.com”.

So if we ask for “sabotage.xelerance.com”, we will get this (signed) NSEC record back

Example DNS zone



```
xelerance.com.  3600    IN      SOA     ns1.xelerance.net. hostmaster.xelerance.com. (
                                        2007110603; Serial
                                        18000   ; refresh
                                        3600    ; retry
                                        864000  ; expire
                                        3600 )  ; minimum
                3600    IN      SSHFP   1 1 023b462a48078fede5328d9bd9e7f1896cef75a7
                3600    IN      SSHFP   2 1 176851637907bffd41d7e161a06d8f2ee14ef35d
                3600    IN      NAPTR   2 0 "s" "SIP+D2T" "" _sip._tcp.xelerance.com.
                3600    IN      NAPTR   2 0 "s" "SIP+D2U" "" _sip._udp.xelerance.com.
                3600    IN      TXT     "v=spf1 ip4:193.110.157.0/24 ~all"
                3600    IN      MX      20 cdc.xelerance.com.
                3600    IN      NS      ns0.xelerance.nl.
                3600    IN      NS      ns1.xelerance.net.
                3600    IN      NS      ns2.xelerance.net.
                3600    IN      A       193.110.157.130
_sip._tcp.xelerance.com.                3600    IN      SRV     1 0 5060 toronto.xelerance.com
_sip._udp.xelerance.com.                3600    IN      SRV     1 0 5060 toronto.xelerance.com
www.xelerance.com.      3600    IN      A       193.110.157.129
```

```
xelerance.com.          3600    IN SOA  ns1.xelerance.net. hostmaster.xelerance.com. (
                                        2007111467 ; serial
                                        18000      ; refresh (5 hours)
                                        3600       ; retry (1 hour)
                                        864000     ; expire (1 week 3 days)
                                        3600       ; minimum (1 hour)
                                        )
                        3600    RRSIG   SOA 5 2 3600 20071214195937 (
                                        20071114195937 18603 xelerance.com.
                                        [...] jEUIl9njngPeeaKtY70yUwiynBI= )
                        3600    NS      ns0.xelerance.nl.
                        3600    NS      ns1.xelerance.net.
                        3600    NS      ns2.xelerance.net.
                        3600    RRSIG   NS 5 2 3600 20071214195937 (
                                        20071114195937 18603 xelerance.com.
                                        dMQbd/p2aXuUhY6gf35SKiaNUfollza6aV/P
                                        [...] +UL5UT0AuGJJXgSEassRy1qxS40= )
                        3600    A       193.110.157.130
                        3600    RRSIG   A 5 2 3600 20071214195937 (
                                        20071114195937 18603 xelerance.com.
                                        F+hzmRkXuKroSwEZNY9MTi9fTrvCSAoV/fut
                                        [...] OYgU4xLdLW1PLMCCdW5VLtbC6d8= )
                        3600    MX      20 cdc.xelerance.com.
                        3600    RRSIG   MX 5 2 3600 20071214195937 (
                                        20071114195937 18603 xelerance.com.
                                        Kyp1/LqifG6ghskHsdGAyYZlysat4Cv2qQfF
                                        [...] PEJ8X01i929E71DosSL/QlyWgoU= )
                        3600    TXT     "Xelerance DNSX Secure Signer version 1.3.1"
                        3600    TXT     "Copyright 2006-2007 Xelerance Corporation"
                        3600    TXT     "v=spf1 ip4:193.110.157.0/24 ~all"
                        3600    RRSIG   TXT 5 2 3600 20071214195937 (
                                        20071114195937 18603 xelerance.com.
                                        D1oW4AiqLLWse2doI3to+Tb4OYPG0QjJo0kc
                                        [...] G568ltcOuLTNd63aaxToV1MZBic= )
```

```
3600    NAPTR   2 0 "s" "SIP+D2T" "" _sip._tcp.xelerance.com.
3600    NAPTR   2 0 "s" "SIP+D2U" "" _sip._udp.xelerance.com.
3600    RRSIG   NAPTR 5 2 3600 20071214195937 (
                20071114195937 18603 xelerance.com.
                nkE6h+NYDzsP1LbuL2gIF7ly5/dnYPQZcxU9
                [...] 0hiHHct3eMSpIdmQlr5Ust5MXXs= )
3600    SSHFP   1 1 (
                023B462A48078FEDE5328D9BD9E7F1896CEF
                75A7 )
3600    SSHFP   2 1 (
                176851637907BFFD41D7E161A06D8F2EE14E
                F35D )
3600    RRSIG   SSHFP 5 2 3600 20071214195937 (
                20071114195937 18603 xelerance.com.
                HtoEKyMMuf1znqddfoTRX13bEdhdgs66rfzB
                [...] WEeN77DL3rPQQrkKWTL/l98y9xg= )
3600    NSEC    _sip._tcp.xelerance.com. A NS SOA MX TXT NAPTR SSHFP
                                         RRSIG NSEC DNSKEY
3600    RRSIG   NSEC 5 2 3600 20071214195937 (
                20071114195937 18603 xelerance.com.
                [...] 4cxQLMtJ4fENvhJkeEGrA3bJsNo= )
3600    DNSKEY  256 3 5 (
                [...] wVSPJmA11HAPrWAC5ncM2o7yCr0sQ7ej
                ) ; key id = 18603
3600    DNSKEY  256 3 5 (
                [...] O+QB00ujCYGO4unk9uVBNYScf2ecGdu7
                ) ; key id = 36522
3600    DNSKEY  257 3 5 (
                [...] 4L43+cudsOfptCXX2FyWQME=
                ) ; key id = 38254
3600    RRSIG   DNSKEY 5 2 3600 20071214195937 (
                20071114195937 18603 xelerance.com.
                [...] a353UzpbmoQcqDLEni1z9kQk49M= )
3600    RRSIG   DNSKEY 5 2 3600 20071214195937 (
                                        20071114195937 18603 xelerance.com.
                                        [...] 4cxQLMtJ4fENvhJkeEGrA3bJsNo= )
                        3600    DNSKEY  256 3 5 (
                                        [...] wVSPJmA11HAPrWAC5ncM2o7yCrOsQ7ej
                                        ) ; key id = 18603
                        3600    DNSKEY  256 3 5 (
                                        [...] O+QB00ujCYGO4unk9uVBNYScf2ecGdu7
                                        ) ; key id = 36522
                        3600    DNSKEY  257 3 5 (
                                        [...] 4L43+cudsOfptCXX2FyWQME=
                                        ) ; key id = 38254
                        3600    RRSIG   DNSKEY 5 2 3600 20071214195937 (
                                        20071114195937 18603 xelerance.com.
                                        [...] a353UzpbmoQcqDLEni1z9kQk49M= )
                        3600    RRSIG   DNSKEY 5 2 3600 20071214195937 (
                                        20071114195937 38254 xelerance.com.
                                        [...] vnB4x1io/7emMKDlJA== )
_sip._tcp.xelerance.com. 3600   IN SRV  1 0 5060 toronto.xelerance.com.
                        3600    RRSIG   SRV 5 4 3600 20071214195937 (
                                        20071114195937 18603 xelerance.com.
                                        [...] sAxnNc4TSgswh9DqwOgHchJo2pY= )
                        3600    NSEC    _sip._udp.xelerance.com. SRV RRSIG NSEC
                        3600    RRSIG   NSEC 5 4 3600 20071214195937 (
                                        20071114195937 18603 xelerance.com.
                                        [...] giqQLG6jbcx6A0F1FnBOpm6Wt48= )
[...]
www.xelerance.com.      3600    IN A    193.110.157.129
                        3600    RRSIG   A 5 3 3600 20071214195937 (
                                        20071114195937 18603 xelerance.com.
                                        [...] o04WzFFhuluhCq5z0vHJXOXoZjU= )
                        3600    NSEC    xelerance.com. A RRSIG NSEC
                        3600    RRSIG   NSEC 5 3 3600 20071214195937 (
                                        20071114195937 18603 xelerance.com.
                                        [...] CRYYfc6pBOUTwxCjckL/dm2Bhww= )
```

The NSEC3 record (draft, not an RFC yet)

Some TLD's (.de and .uk) did not like the fact that you can discover all data in the DNS by “walking the NSEC” record chain

Use sorted hashed names instead

The NSEC3 record

```
2t7b4g4vsa5smi47k61mv5bv1a22bojr.example.com.
       NSEC3   1 1 12 aabbccdd (
            2vptu5timamqttgl4luu9kg21e0aor3s A RRSIG)
```

If we want the A record for “www.example.com” and we get this NSEC3 record back, we calculate hash(record,salt,interations) falls between “2t7b4g[...]” and “2vptu5[...]”.

If hash(“www.example.com”,”aabbccdd”,12) is “2uaaa[...]” then we have a signed answer that an A record for “www.example.com” does not exist, without knowing any other hostname in the zone.

.com: All or Nothing?

Problem: We need DNSSEC deployment yesterday

No large TLD's, like .com, .org, .uk, .ge or .eu are going to enable DNSSEC tomorrow.

But we want to protect our entries within those zones now (eg xelerance.com)

How can migrate from DNS to DNSSEC ?

We need a list of DNSSEC domains

For each domain in an non-DNSSEC TLD, we keep a database with their DNSKEY

Resolvers need to check for DNSSEC on the TLD, and when in a non-DNSSEC TLD, query our database.

We require this database to be as reliable as the DNS itself.

We require this database to be as secure as DNSSEC

Hmm....database....distributed.....needs crypto......

I know, let's use the DNS

DNSSEC Lookaside Verification

xelerance.com.dlv.isc.org. IN DLV 38254 5 1
77F7CAEAA4547DB69F6F563CE7A164558E8C1

See: http://dlv.isc.org/

Other issues not discussed here

Versign wants “opt-in”, meaning they want NSEC or NSEC3 records to skip unsigned data. This would allow them to only have limited signed data for signed domains, instead of having to sign the entire com/net zone from day 1.

Wildcard records. Those records match a lot (eg: *.many.example.com). Those are also covered properly by NSEC or NSEC3 records.

Hash agility for NSEC3. There is no method for switching hash functions, other then to first fall back to NSEC.

Signed data validity

To prevent replay attacks, cryptographically signed data must “expire” and new signed data must be created. Hence the start and end date in the RRSIG records.

DNS data has a “time to live” to allow DNS caching.

So updating signed data always needs to happen with some overlap in time of DNSKEY records

Key rollover

Cryptograhic keys need to be replaced regularly
Cryptographic algorithms might have to be replaced
Cryptographic keys can get compromised or lost

We need a mechanism to migrate from old to new key

DNS data has a “time to live” to allow DNS caching. We need to keep the old key around for a little while even if we have purged all signatures of the old key
The DS record might be cached as well, and point to the old key (and we prefer not to require two DS records at the parent)

Required feature set for DNSSEC

DNSSEC operations

- Key Signing Keys and Zone Signing Keys management
- Zone signing and re-signing management
- Key rollover management (KSK and ZSK)
- Emergency key rollover support
- DNSSEC Lookaside Verification (DLV) support eg: dlv.isc.org

DNSSEC and DNS records management

- DS record management (fully automatic if we are parent and child)
- DS record support on external parent (point to proper TLD pages)
- System wide and per-domain DNSSEC settings for key types, key sizes, signature lifetime, re-sign interval

Key rollover method

Current DNSKEY (A) plus Future DNSKEY (B)
Parent publishes DS(A)

Old DNSKEY (A) plus Current DNSKEY (B)
Parent publishes DS(B)

Current DNSKEY (B) plus Future DNSKEY (C)
Parent publishes DS(B)

All wait times depend on TTL of RRSIG and DNSKEY's
All wait times depend on interaction with parent for DS

Decrease parent-child interaction

Publish one “Master DNSKEY”

- Strong key strength (2048 bit)
- Long lived key (one year validity)
- Send DS of master key to parent
- Yearly rollover as described on previous slide

Publish one “Zone DNSKEY”

- Reasonable key strength (1024bit)
- Short lived key (30 days)
- Zone key is signed by “Master DNSKEY”
- Key can be updated without updating DS record

Trust path is now:

DS(Master) -> Master -> Sig(Zone key) -> Sig (zone data)

The DNSSEC difference

DNS

Fairly straightforward simple concept

Setup once and forget about it – easy to pickup

Forgiving for human errors

Integrated differently with each organisation, usually features webgui and db

Data never expires,delays with nameservers not critical

Core standard everywhere

DNSSEC

Conceptually hard for average zone admin

Continuous effort required to maintain signed zones

Human errors have dire consequences.

Does not fit in currently deployed DNS infrastructure

Data becomes stale, smooth integration with nameserver required

Non-uniform deployment

Required feature set for DNSSEC

DNSSEC operations

- Key Signing Keys and Zone Signing Keys management
- Zone signing and re-signing management
- Key rollover management (KSK and ZSK)
- Emergency key rollover support
- DLV support – standard configuration uses dlv.isc.org

DNSSEC and DNS records management

- DS record management (fully automatic if we are parent and child)
- DS record support on external parent (point to proper TLD pages)
- System wide and per-domain DNSSEC settings for key types, key sizes, signature lifetime, re-sign interval

Desired features for DNSSEC

Automation support

All features except “DS upload to external parent” can be automated but the tools are not ready yet.

IETF with ISC is working on automating DS record trust

Nameserver integration

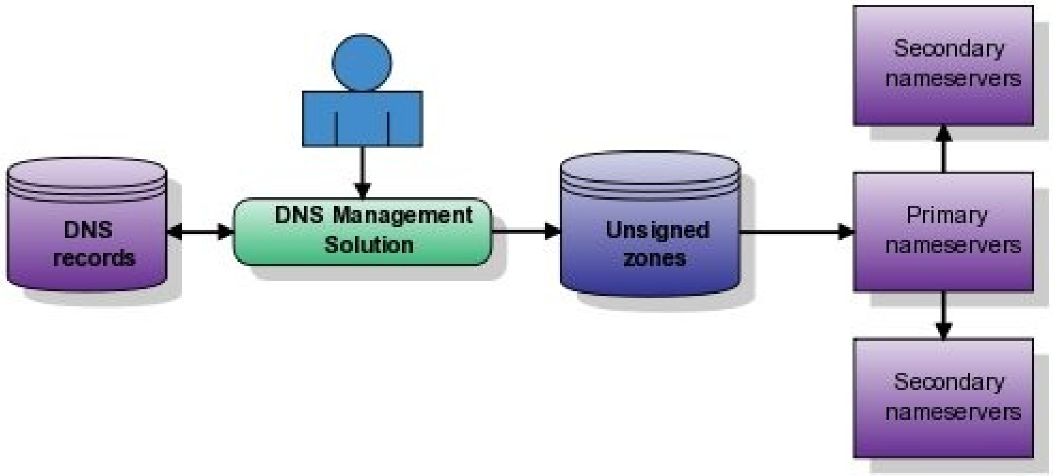
Due to timing sensitivities, a DNSSEC signer needs to be fully integrated into the nameserver for automated zone uploads.

Online mode or Offline mode (features vs security)

Active verification of DNSSEC records, zones and nameservers

Notification of imminent or occurring issues

Typical DNS Deployment

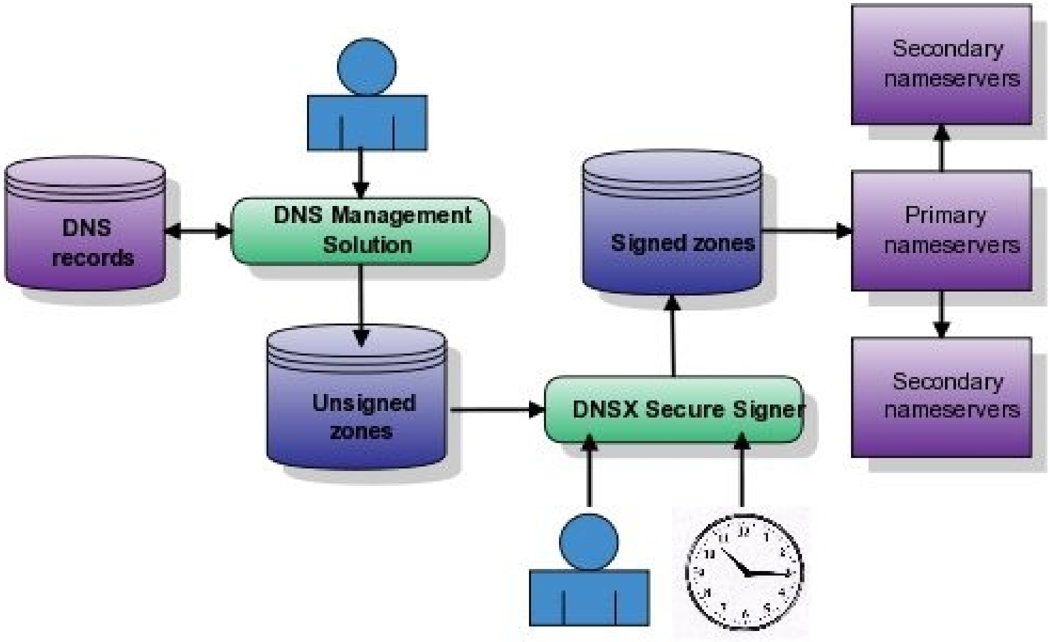


dnssec solution should be a drop-in solution

dnssec solution should integrate with all existing DNS management solutions without requiring infrastructure changes

Provide one-step fallback scenario

DNSSEC integration example



Needs to push signed zones via SSH, SFTP, NFS or SMB
Needs to support custom (**ssh?)** reload command

/usr/sbin/rndc reload
/etc/init.d/nsd restart
touch /var/dns/queue/do-ns-restart

Resolving DNSSEC

Available software

- ISC Bind 9 nameserver
  - DNSSEC authorative nameserver
  - DNSSEC recursing nameserver
  - DNSSEC signer
  - DNSSEC DLV support
- NSD nameserver
  - DNSSEC authorative nameserver
- dnssec-tools.org
  - DNSSEC signer management tool
  - DNSSEC library
- www.ripe.net/disi/
  - DNSSEC signer management tool in perl
- ldns
  - Unix dnssec library in C.

Create signed zone mini-HOWTO

```
dnssec-keygen -r /dev/random -f KSK -a
  RSASHA1 -b 2048 -n ZONE example.com

dnssec-keygen -r /dev/random  -a RSASHA1
  -b 1024 -n ZONE example.com

dnssec-signzone  -l dlv.isc.org -r /dev/random
  -o example.com -k \
  Kexample.com.+005+aaaaa example.com
  Kexample.com.+005+bbbbb.key
```

Create Secure Resolver HOWTO 1

named.conf – options section

```
// On Redhat/Fedora Bind, they created a new option
// edns yes;

dnssec-enable yes;
dnssec-validation yes;
dnssec-accept-expired no;

// For DNSSEC Lookaside Verifcation
dnssec-lookaside . trust-anchor dlv.isc.org.;
```

Create Secure Resolver HOWTO 2

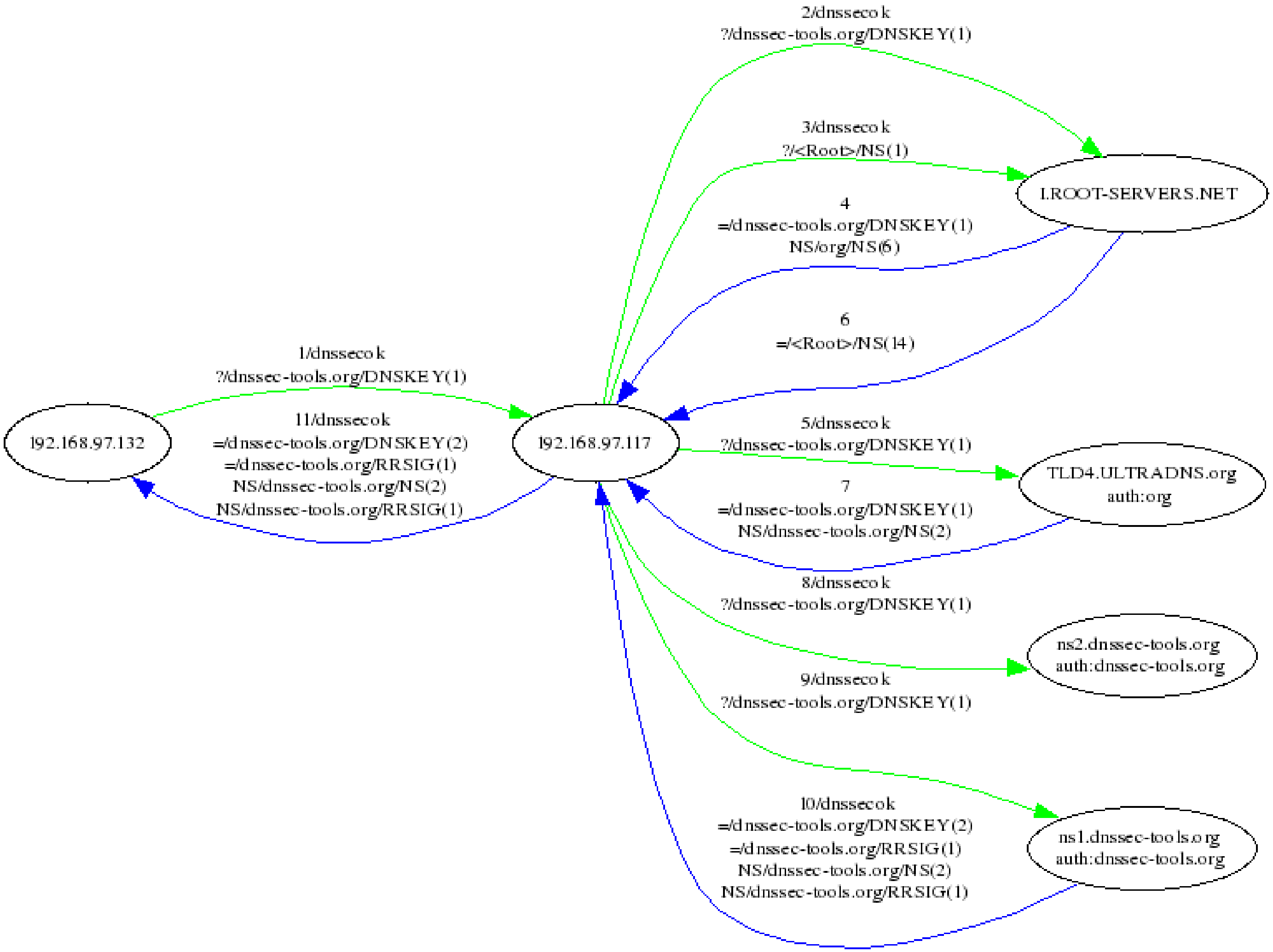
named.conf – Add your DNSKEY:

```
trusted-keys {
"xelerance.com." 257 3 5
  "AwEAAcat1tpsyH hVU3EcezXG 5dUWDKgo
   52u75gp0TXfE+gwPJ fr8PYAs+1ankqKlJ54d
   GWwwzH10DplxfB3 AgovMdkgVnQiNp/LR7Z
   gmA7nYWDqhRdY ZUL0WEhKaXF5qed9eJA
   Jy4clyePTSx6Jd iGWQadbce9tKwWFdabhWg
   cforlmONxw71B21 Q9UMHIVmPZFXjX20yN4
   xYc8dql51zFNU1 d2E7bUcZ14GsXN5DuyPub
   WUJ4r7TNiUqYwvGP K+p8HK5Tqxa1W73dR
   g6VZZ0aZxHOJnLfT Qu0ejDHvq5La5ZUfdb
  4L43+cudsOfptC XX2FyWQME="; // key id = 38254
};
```

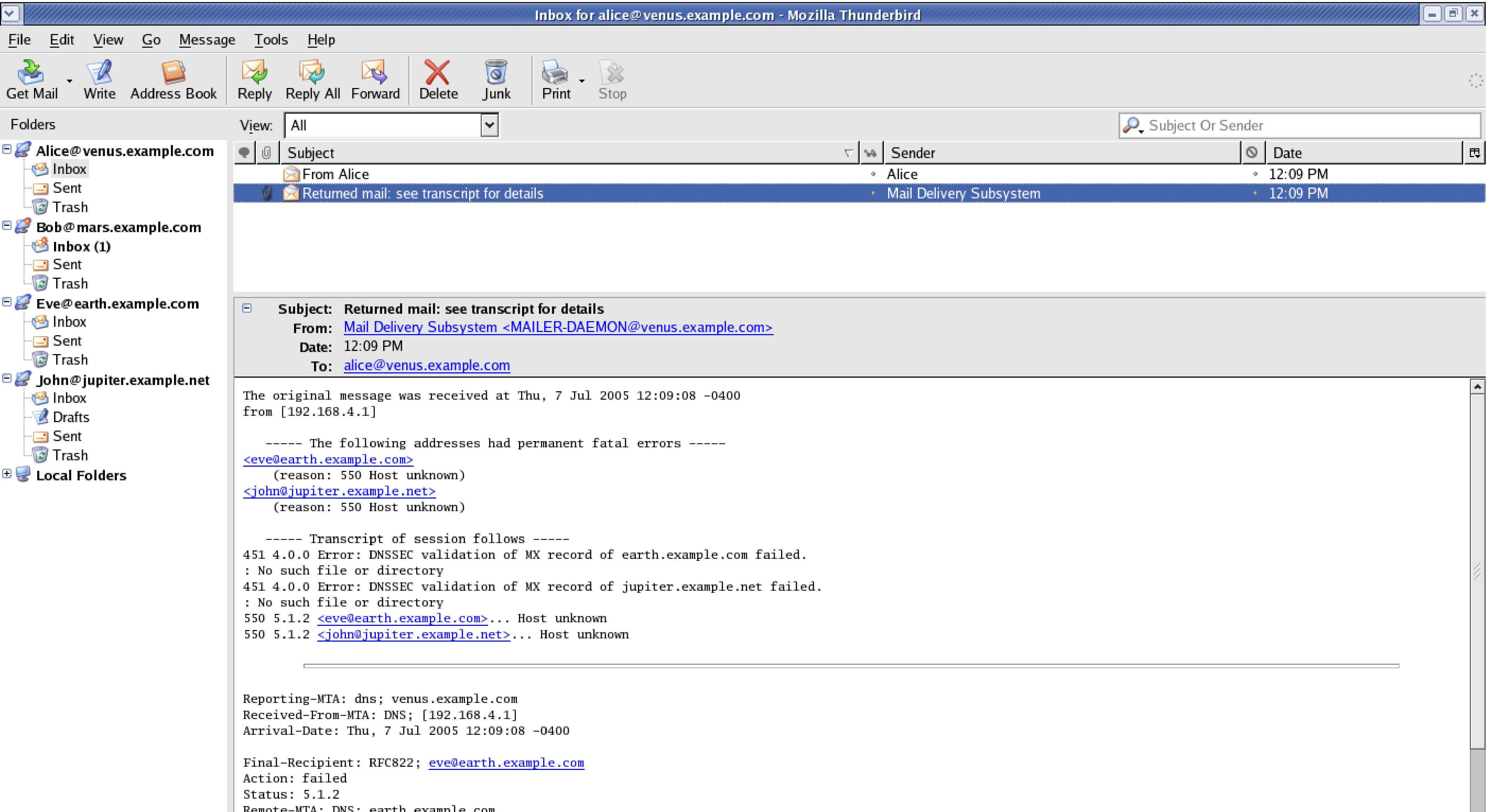
Available DNSSEC aware applications

dnssec-tools.org added DNSSEC to a few very important applications !!

dnssec-tools.org: Visualisation tools


192.168.97.132
192.168.97.117
I.ROOT-SERVERS.NET
TLD4.ULTRADNS.org
auth:org
ns2.dnssec-tools.org
auth:dnssec-tools.org
ns1.dnssec-tools.org
auth:dnssec-tools.org
1/dnssecok
?/dnssec-tools.org/DNSKEY(1)
11/dnssecok
=/dnssec-tools.org/DNSKEY(2)
=/dnssec-tools.org/RRSIG(1)
NS/dnssec-tools.org/NS(2)
NS/dnssec-tools.org/RRSIG(1)
2/dnssecok
?/dnssec-tools.org/DNSKEY(1)
3/dnssecok
?/<Root>/NS(1)
4
=/dnssec-tools.org/DNSKEY(1)
NS/org/NS(6)
6
=/<Root>/NS(14)
5/dnssecok
?/dnssec-tools.org/DNSKEY(1)
7
=/dnssec-tools.org/DNSKEY(1)
NS/dnssec-tools.org/NS(2)
8/dnssecok
?/dnssec-tools.org/DNSKEY(1)
9/dnssecok
?/dnssec-tools.org/DNSKEY(1)
10/dnssecok
=/dnssec-tools.org/DNSKEY(2)
=/dnssec-tools.org/RRSIG(1)
NS/dnssec-tools.org/NS(2)
NS/dnssec-tools.org/RRSIG(1)

dnssec-tools.org
POSTFIX and Sendmail



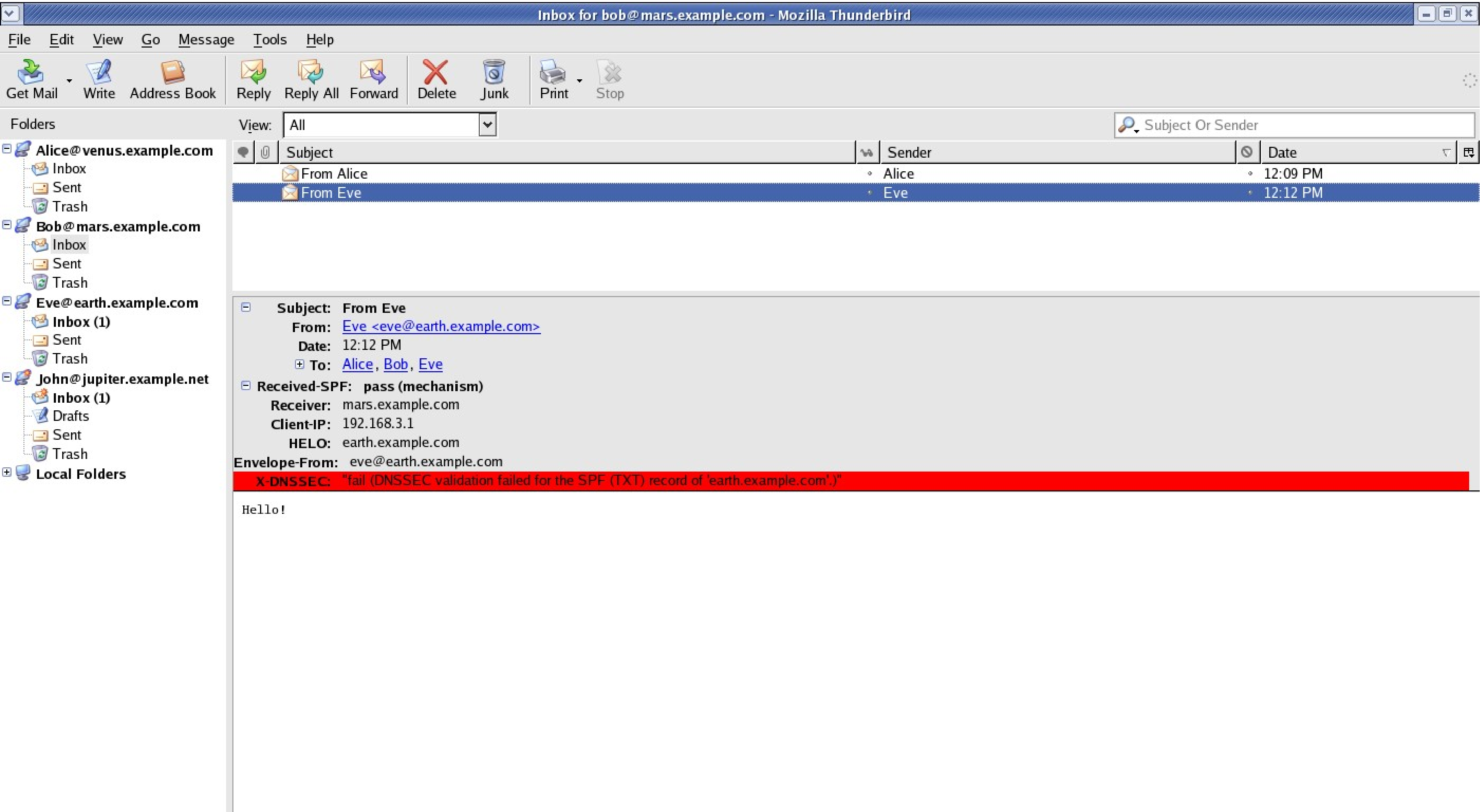
Subject	Sender	Date
From Alice	Alice	12:09 PM
Returned mail: see transcript for details	Mail Delivery Subsystem	12:09 PM

Subject: Returned mail: see transcript for details
From: Mail Delivery Subsystem <MAILER-DAEMON@venus.example.com>
Date: 12:09 PM
To: alice@venus.example.com

```
The original message was received at Thu, 7 Jul 2005 12:09:08 -0400
from [192.168.4.1]

   ----- The following addresses had permanent fatal errors -----
<eve@earth.example.com>
    (reason: 550 Host unknown)
<john@jupiter.example.net>
    (reason: 550 Host unknown)

   ----- Transcript of session follows -----
451 4.0.0 Error: DNSSEC validation of MX record of earth.example.com failed.
: No such file or directory
451 4.0.0 Error: DNSSEC validation of MX record of jupiter.example.net failed.
: No such file or directory
550 5.1.2 <eve@earth.example.com>... Host unknown
550 5.1.2 <john@jupiter.example.net>... Host unknown
```

```
Reporting-MTA: dns; venus.example.com
Received-From-MTA: DNS; [192.168.4.1]
Arrival-Date: Thu, 7 Jul 2005 12:09:08 -0400

Final-Recipient: RFC822; eve@earth.example.com
Action: failed
Status: 5.1.2
Remote-MTA: DNS; earth.example.com
```

dnssec-tools.org Thunderbird mail client

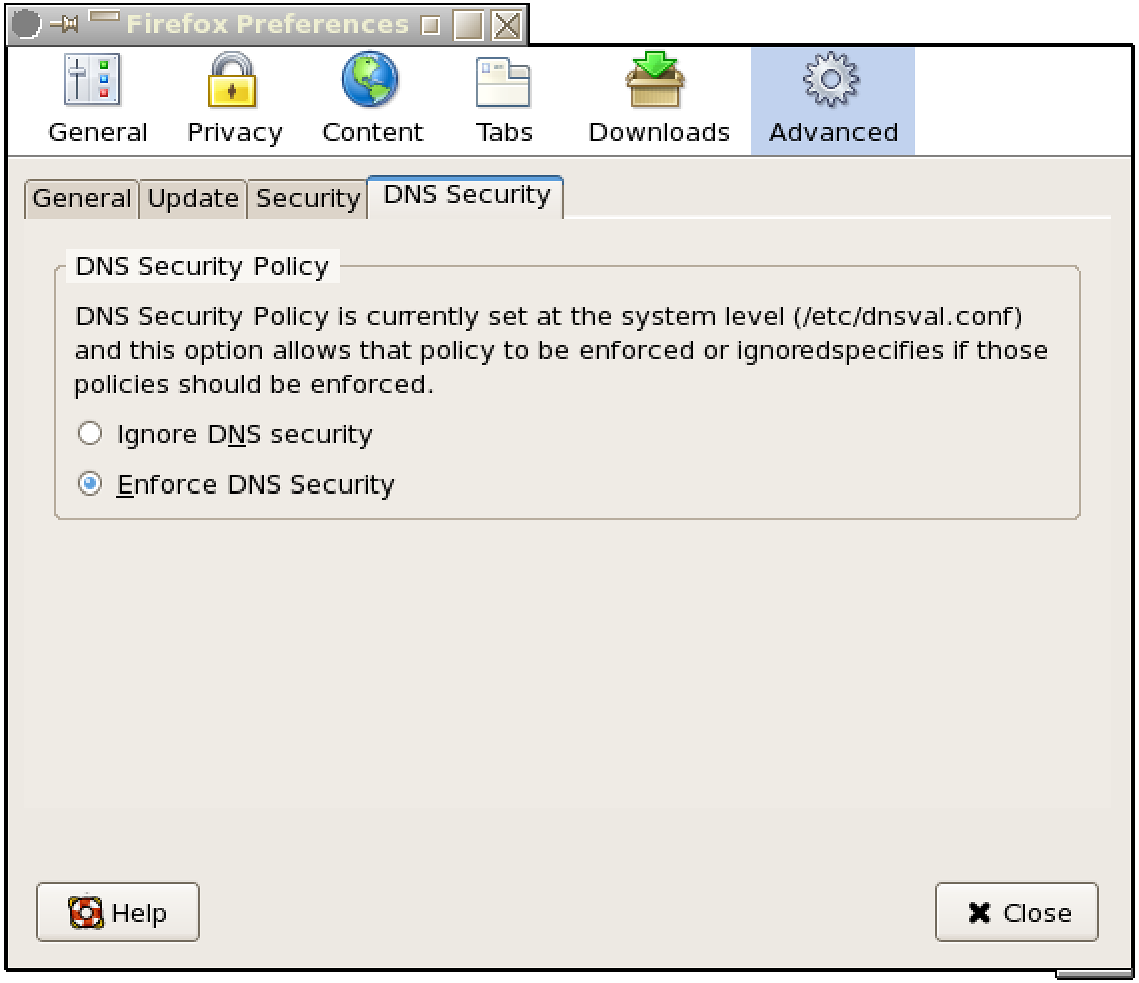


Subject	Sender	Date
From Alice	Alice	12:09 PM
From Eve	Eve	12:12 PM

Subject: From Eve
From: Eve <eve@earth.example.com>
Date: 12:12 PM
To: Alice, Bob, Eve
Received-SPF: pass (mechanism)
Receiver: mars.example.com
Client-IP: 192.168.3.1
HELO: earth.example.com
Envelope-From: eve@earth.example.com
X-DNSSEC: "fail (DNSSEC validation failed for the SPF (TXT) record of 'earth.example.com'.)"

```
Hello!
```

dnssec-tools.org
Firefox web browser



DNS Security Policy

DNS Security Policy is currently set at the system level (/etc/dnsval.conf) and this option allows that policy to be enforced or ignoredspecifies if those policies should be enforced.

○ Ignore DNS security

● Enforce DNS Security

NLnetlabs Firefox plugin

[demo]

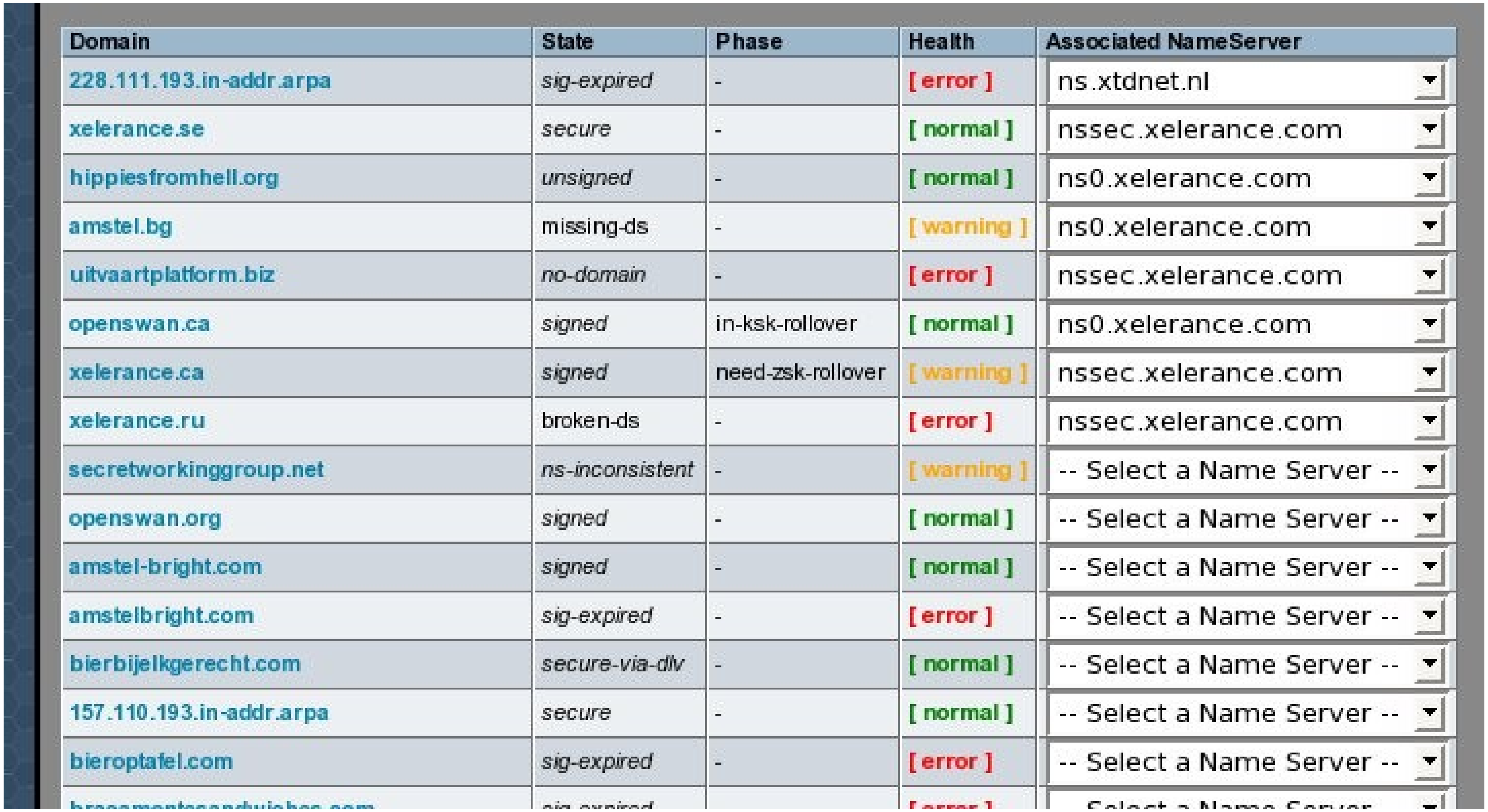
Conclusion

DNSSEC has been deployed and will gain widespread deployment by cc:TLD's in the next year

Walk, don't run, to deploying DNSSEC

Xelerance DNSX Secure Signer

Xelerance DNSX Secure Signer Screenshot



Domain	State	Phase	Health	Associated NameServer
228.111.193.in-addr.arpa	*sig-expired*	-	[error]	ns.xtdnet.nl
xelerance.se	secure	-	[normal]	nssec.xelerance.com
hippiesfromhell.org	*unsigned*	-	[normal]	ns0.xelerance.com
amstel.bg	missing-ds	-	[warning]	ns0.xelerance.com
uitvaartplatform.biz	*no-domain*	-	[error]	nssec.xelerance.com
openswan.ca	*signed*	in-ksk-rollover	[normal]	ns0.xelerance.com
xelerance.ca	*signed*	need-zsk-rollover	[warning]	nssec.xelerance.com
xelerance.ru	broken-ds	-	[error]	nssec.xelerance.com
secretworkinggroup.net	*ns-inconsistent*	-	[warning]	-- Select a Name Server --
openswan.org	*signed*	-	[normal]	-- Select a Name Server --
amstel-bright.com	*signed*	-	[normal]	-- Select a Name Server --
amstelbright.com	*sig-expired*	-	[error]	-- Select a Name Server --
bierbijelkgerecht.com	*secure-via-dlv*	-	[normal]	-- Select a Name Server --
157.110.193.in-addr.arpa	secure	-	[normal]	-- Select a Name Server --
bieroptafel.com	*sig-expired*	-	[error]	-- Select a Name Server --
[illegible]	*sig-expired*		[error]	-- Select a Name Server --