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

Xelerence Corporation is heavily 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 hierarchical and distributed

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

HTTP://NIRLOG.COM/2006/03/28/DNS-AMPLIFICATION-ATTACK/

Step 1
Question: what is the IP Address of some-webserver.com?
Answer: Here is the IP Address of some-webserver.com.

Step 2
Question: where can I find the IP Address of some-webserver.com?
Answer: I don't know but .com NameSpace should have the answer.

Step 3
Not authoritative for some-webserver.com.

Step 4
Question: What is the IP Address of some-webserver.com?
Answer: Primary DNS Server of some-webserver.com knows it.

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

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

Step 7
Primary DNS Server of some-webserver.com.

Step 8
User's Primary DNS Server (Recursion Allowed)

Root Servers

.DNS Query (Recursive)
(by Nirlog.com)

User's PC
My IP Address
15 attacks on DNS

It takes a lot of queries to get an answer

[ let me show you.... ]
Attack 1
Endpoint DNS spoofing
Attack 2
ISP cache poisoning, then spam

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

Localised attack by remote attacker

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 behalf 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)

google.com -> google.com

But what if google.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!
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
Attack 10
NXDOMAIN thieves [part 2]

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

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


(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)
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.
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 Threat Analyses” by Santcroos, Kolkman

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 in DNS. 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 were not larger than 512 bytes, but DNS packets with EDNS0 can be larger than 512 bytes.


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 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 thwarted. 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 Nameservers: 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

This map was created by Paul Wouters

Production ccTLD
Production Reverse
Testbed
Discontinued
gTLDs/DLV Testbeds

Production ccTLD'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.
DNSSEC survey by ccNSO Council
October 27 2007 65 ccTLD's responded

Have you implemented DNSSEC?

- YES 7%
- NO 86%
- Test version 5%
- Other 2%
DNSSEC survey by ccNSO Council
October 27 2007        65 ccTLD's responded

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

- YES 85%
- NO 10%
- Unsure 6%
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?

- Lack of resources
- Waiting for DNSSEC to mature
- Other projects have higher priority
- Root Zone not signed
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?

![Bar chart showing percent of respondents for different timelines: Within 1 year (35%), 2 years (10%), 3 years (25%), No set timeline (20%)]
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 separate
  bind – fully implemented (including 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 (AwEAAamc7W2EQdv34ZyUFapilEzOmcxZE8YQvJ3o1L+QdWU0O7VspH5iNXE16bWrez7tOHBPZfxsJYurF0GQMXQ+kVh0Ls0uPyhvQkE+arcQhXG2scCDPIBmD0iuVx50+qBN90QnXmESoywVSPJmA11HAPrAC5ncM2o7yCrOsQ7ej)

) ; 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
vgDPy26pFhztdEcx9hXiXSVX15Hh4jlxEJNr
M8A61HZftIV3ujr8CwfPLf3BD6nJVjEt+Xxs
FxWFOd01co04WzFFhuluwCq5z0vHJXOX
oZjU= )
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 infinite 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 86400; expire 3600; minimum

3600 IN SSHFP 1 1 023b462a48078fede5328d9bd9e7f1896cef75a7
3600 IN SSHFP 2 1 176851637907bffdf41d7e161a06d8f2ee14ef35d
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
Example DNSSEC zone

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 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
[...] 0YgU4xLdLW1PLMCCdW5VLtbG6d8= )

3600 MX 20 cdc.xelerance.com.
3600 RRSIG MX 5 2 3600 20071214195937
(20071114195937 18603 xelerance.com.
Kyp1/LqifG6ghskHsdGAYZlysat4Cv2qQfF
[...] PEJ8X011929E71DosSL/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 TXT 5 2 3600 20071214195937
(20071114195937 18603 xelerance.com.
DiOw4AiqLLwse2doI3to+Tb40YPG0QjJo0kc
[...] G568ltcOuLTNd63aaxToV1MZBi= )
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.
   nkJmE6h+NYDzsP1LbuL2gIF7ly5/dnYPQZcxU9
   [...] 0hiHHct3eMSpIdmQlr5Ust5MXXs= )
3600 SSHFP 1 1 (023B462A48078FDE5328D9BD9E7F1896CEF75A7)
3600 SSHFP 2 1 (176851637907BFFE41D7E161A06D8F2EE14E035D)
3600 RRSIG SSHFP 5 2 3600 20071214195937 (20071114195937 18603 xelerance.com.
   HtoEkyMMuf1zngdfoTRX13bEdhdgs66rZfB
   [...] WZen77DL3rPQQrKWTL/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.
   [...] 4cxQLMtJ4fENvJkeEGrA3bJsNo= )
3600 DNSKEY 256 3 5 (wVSPJmAl1HAPrWAC5ncMzo7yCr0sQ7ej
   ) ; key id = 18603
3600 DNSKEY 256 3 5 (0+QB00ujCYG04unk9uVBNYScf2ecGdu7
   ) ; key id = 36522
3600 DNSKEY 257 3 5 (4L43+cudsOfptCXX2FyWQME=
   ) ; key id = 38254
3600 RRSIG DNSKEY 5 2 3600 20071214195937 (20071114195937 18603 xelerance.com.
   [...] a353UzpBmoQcqDLEnl1z9kQk49M= )
3600 RRSIG DNSKEY 5 2 3600 20071214195937 (
20071114195937 18603 xelerance.com

DNSKEY 3600
256 3 5 ( 
... 4cX0Mj4fENvHKeEGrA3bJsNo= )
key id = 18603

DNSKEY 3600
256 3 5 ( 
... wVSPjA11HAPrWAC5ncM2o7yCr0s07e7 )
key id = 36522

DNSKEY 3600
257 3 5 ( 
... 0+Q80uJCYG04unk9uVBNYScf2ecGdu7 )
key id = 38254

RRSIG 3600
DNSKEY 5 2 3600 20071114195937 ( 
20071114195937 18603 xelerance.com.
... a353UzpbmoQcDLEni1z9kQk49M= )

RRSIG 3600
DNSKEY 5 2 3600 20071114195937 ( 
20071114195937 38254 xelerance.com.
... vNB4xli0/7emMKDLJA= )

_sip._tcp.xelerance.com. 3600 IN SRV 1 0 5060 toronto.xelerance.com.

SRV 3600
5 4 3600 20071114195937 ( 
20071114195937 18603 xelerance.com.
... sAXnNc4TSgswh9Dqw0hChJo2pY= )

_NSEC 3600
_sip._udp.xelerance.com. SRV RRSIG NSEC

RRSIG 3600
NSEC 5 4 3600 20071114195937 ( 
20071114195937 18603 xelerance.com.
... giqQLG6jbcx6A0F1FmBo6Wt48= )

3600 IN A 193.110.157.129

A 3600
5 3 3600 20071114195937 ( 
20071114195937 18603 xelerance.com.
... oS4WzFHuluGq5z0vHXOxOZjU= )

NSEC 3600
xelerance.com. A RRSIG NSEC

NSEC 3600
5 3 3600 20071114195937 ( 
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 aabbccddd (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”,”aabbccddd”,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

Cryptographic 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
- 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 authoritative nameserver
  - DNSSEC recursing nameserver
  - DNSSEC signer
  - DNSSEC DLV support
- NSD nameserver
  - DNSSEC authoritative 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+bbbbbb.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 Verification
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 Q9UMHIvMnPzFxjX20yN4
xYc8dql51zFNU1 d2E7bUcZ14GsXN5DuyPub
WUJ4r7TNiUqYwvGP K+p8HK5Tqxa1W73dR
g6VZZ0aZxHOJnLdT 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
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)
<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 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
 dnssec-tools.org
Thunderbird mail client

Hello!
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 ignored. Specifies 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

<table>
<thead>
<tr>
<th>Domain</th>
<th>State</th>
<th>Phase</th>
<th>Health</th>
<th>Associated NameServer</th>
</tr>
</thead>
<tbody>
<tr>
<td>228.111.193.in-addr.arpa</td>
<td>sig-expired</td>
<td></td>
<td>[error]</td>
<td>ns.xtdnet.nl</td>
</tr>
<tr>
<td>xelerance.se</td>
<td>secure</td>
<td></td>
<td>[normal]</td>
<td>nssec.xelerance.com</td>
</tr>
<tr>
<td>hippiesfromhell.org</td>
<td>unsigned</td>
<td></td>
<td>[normal]</td>
<td>ns0.xelerance.com</td>
</tr>
<tr>
<td>amstel.bg</td>
<td>missing-ds</td>
<td></td>
<td>[warning]</td>
<td>ns0.xelerance.com</td>
</tr>
<tr>
<td>uitvaartplatform.biz</td>
<td>no-domain</td>
<td></td>
<td>[error ]</td>
<td>nssec.xelerance.com</td>
</tr>
<tr>
<td>openswan.ca</td>
<td>signed</td>
<td>in-ksk-rollover</td>
<td>[normal]</td>
<td>ns0.xelerance.com</td>
</tr>
<tr>
<td>xelerance.ca</td>
<td>signed</td>
<td></td>
<td>[warning]</td>
<td>nssec.xelerance.com</td>
</tr>
<tr>
<td>xelerance.ru</td>
<td>broken-ds</td>
<td></td>
<td>[error ]</td>
<td>nssec.xelerance.com</td>
</tr>
<tr>
<td>secretworkinggroup.net</td>
<td>ns-inconsistent</td>
<td></td>
<td>[warning]</td>
<td>-- Select a Name Server --&gt;</td>
</tr>
<tr>
<td>openswan.org</td>
<td>signed</td>
<td></td>
<td>[normal]</td>
<td>-- Select a Name Server --&gt;</td>
</tr>
<tr>
<td>amstel-bright.com</td>
<td>signed</td>
<td></td>
<td>[normal]</td>
<td>-- Select a Name Server --&gt;</td>
</tr>
<tr>
<td>amstelbright.com</td>
<td>sig-expired</td>
<td></td>
<td>[error ]</td>
<td>-- Select a Name Server --&gt;</td>
</tr>
<tr>
<td>bierbijelkgerecht.com</td>
<td>secure-via-dlv</td>
<td></td>
<td>[normal]</td>
<td>-- Select a Name Server --&gt;</td>
</tr>
<tr>
<td>157.110.193.in-addr.arpa</td>
<td>secure</td>
<td></td>
<td>[normal]</td>
<td>-- Select a Name Server --&gt;</td>
</tr>
<tr>
<td>bieroptafel.com</td>
<td>sig-expired</td>
<td></td>
<td>[error ]</td>
<td>-- Select a Name Server --&gt;</td>
</tr>
<tr>
<td>beermeetboardvrijes.com</td>
<td>sig-expired</td>
<td></td>
<td>[error ]</td>
<td>-- Select a Name Server --&gt;</td>
</tr>
</tbody>
</table>