



Black Hat[®]

Europe 2003

Deploying DNSSEC

By Paul Wouters
<paul@xtdnet.nl>



Black Hat®

Europe 2003

Deploying DNSSEC

Overview presentation

- Theory of DNSSEC
- Using bind with DNSSEC
- Securing “.nl” with SECREG
- Securing “.org” with VerisignLabs
- Deploying DNSSEC on large scale
- Audience participation (hack my DNSSEC)



Black Hat[®]

Europe 2003

Deploying DNSSEC

Server view of DNS

<IMAGE>



Black Hat®

Europe 2003

Deploying DNSSEC

Zone view of DNS

From Answer	To	Question	
Clientip	Resolver	A www.freeswan.nl	193.110.157.9
<file>	-	NS .	NS
A.ROOT-SERVERS.NET.			A
198.14.0.4 (GLUE)			
Resolver	198.14.0.4	NS nl.	NS
NS.DOMAIN-REGISTRY.NL			A
193.176.144.2 (GLUE)			
Resolver	193.176.144.2	NS freeswan.nl.	NS ns.xtdnet.nl.
			A
193.110.157.2 (GLUE)			
Resolver	193.110.157.2	A www.freeswan.nl.	A 193.110.157.9

(AUTHORITATIVE)



Black Hat®

Europe 2003

Deploying DNSSEC

Organisational view of DNS

- The Root Registry (InterNic/VeriSign/DoD/IANA/IAB/ICANN)
- ROOT-SERVERS.NET (IETF)
- CC:TLD-SERVERS.NET (IETF/RIPE/RIPE NCC)
- The NL Registry DOMAIN-REGISTRY.NL (SIDN)
- (AMS-IX,KPN,NIKHEF,SURFNET,RIPE NCC,NIC.SE,NIC.FR,UUNET)
- Registrar of 157.110.193.IN-ADDR.ARPA. (XTDNET,RIPE,BBC)
- ISP of 157.110.193.IN-ADDR.ARPA. (XTDNET,BBC,EASYNET,INTERNATION)
- Registrant (FreeS/WAN)

- **23** Organisations (+everyone with access to routing or BL tables)



Deploying DNSSEC

Vulnerabilities of DNS:

- 1) Integrity of data
- 2) Authenticity of data

- _ Client <-> DHCP Server
- _ Client <-> Resolver
- _ Resolver itself (rootfile)
- _ Resolver's communication to the net
- _ Various glue records and their update mechanism
- _ Various nameserver <-> nameserver communication
- _ Various network <-> network communication



Black Hat®

Europe 2003

Deploying DNSSEC

Protect DNS with digital signatures

- _ Secure client <-> resolver communication
 - Secure LAN/DHCP?
 - DNSSEC aware Resolver on Client?
- _ Secure communication nameservers
 - Zone transfers (AXFR)
 - dynamic updates
- _ Secure data storage integrity
 - Zonefiles
 - Caches



Black Hat®

Europe 2003

Deploying DNSSEC

Secure nameserver communication

- _ TSIG: Preshared Secret Key to protect AXFR
 - Strictly speaking not necessary with secure zones
 - Secure the IP layer
 - . IPsec tunnel between master and slaves
 - . Transfer zones from master to slave using SSH/SCP/SFTP
- _ SIG0: Public key cryptography
 - See above
 - Useful for dynamic updates



Black Hat®

Europe 2003

Deploying DNSSEC

DNSSEC: The new record types

- _ The KEY record: The public key used
- _ The SIG record: The signatures created by the key
- _ The NXT record: For denial of existence
- _ The DS record: For building the chain of trust

- _ New flag: The Authenticated Data (AD) flag
 - _ Not protected by a signature!



Black Hat®

Europe 2003

Deploying DNSSEC

DNSSEC: The KEY record

```
Rlabel TTL IN KEY <flags> <protocol> <algorithm> <key material>
```

```
reeswan.nl. 3600 IN KEY 256 3 5 (  
    AQPRv8TN8ayfxrtRo1dveOMVSSpT4PGEZvfGjaERldQZ  
    izYKgVBj/l84DjVktGUbkJ3pBiLBAzZ+5nbGkWn+Lz5Z  
    HMIQnjWde/mKKDIZnwQ13vU+HPt3cszNy9CdBmn6l8=  
    ) ; key id = 56954
```

Flags: authentication, confidentiality

Protocol: DNSSEC = 3. IPsec = 4



Black Hat®

Europe 2003

Deploying DNSSEC

DNSSEC: The NXT record

```
Rlabel TTL IN NXT <alphanumeric next Rlabel>  
                        <list of existing RRsets>
```

```
freeswan.nl. 3600 IN NXT activeOE.freeswan.nl. NS SOA MX SIG KEY  
NXT
```

Denial of existence: We now know there is no RRset abc.freeswan.nl.



Black Hat®

Europe 2003

Deploying DNSSEC

DNS: Example zone

```
$TTL 3600
freeswan.nl.      IN      SOA     ns.xtdnet.nl. hostmaster.freeswan.nl. (
                  2003040619 ; Serial
                  28800   ; Refresh
                  7200    ; Retry
                  604800  ; Expire
                  3600)   ; Minimum

freeswan.nl.      IN      NS     ns.xtdnet.nl.
freeswan.nl.      IN      NS     ns1.xtdnet.nl.
www.freeswan.nl.  IN      A      193.110.157.9
freeswan.nl.      IN      MX     50      www.freeswan.nl.
                                      1,1      All
```



Black Hat®

Europe 2003

Deploying DNSSEC

```
freeswan.nl. 3600 IN SOA ns.xtdnet.nl. hostmaster.freeswan.nl. (
2003040620 ; serial
28800 ; refresh (8 hours)
7200 ; retry (2 hours)
604800 ; expire (1 week)
3600 ; minimum (1 hour)
)
3600 SIG SOA 5 2 3600 20030510221048 (
20030410221048 56954 freeswan.nl.
[...] HVEb/ksXy/vNrY3JKVoo )
3600 NS ns.xtdnet.nl.
3600 NS ns1.xtdnet.nl.
3600 SIG NS 5 2 3600 20030510221048 (
20030410221048 56954 freeswan.nl.
[...] ePuHDsDldZwDX1lcha+j )
3600 MX 50 www.freeswan.nl.
3600 SIG MX 5 2 3600 20030510221048 (
20030410221048 56954 freeswan.nl.
[...] a1MzpY1wx09AWoyNIf/g )
3600 KEY 256 3 5 (
[...] FSc6wWff2MSuG9qZ6o1H
) ; key id = 49601
3600 KEY 256 3 5 (
[...] 13vU+HPt3cszNy9CdBmn618=
) ; key id = 56954
3600 SIG KEY 5 2 3600 20030510221048 (
20030410221048 49601 freeswan.nl.
[...] Lzktbwf51H1qD+sQ3w== )
3600 SIG KEY 5 2 3600 20030510221048 (
20030410221048 56954 freeswan.nl.
[...] G/z+MdVYVsafdmXgh9+0 )
3600 NXT www.freeswan.nl. NS SOA MX SIG KEY NXT
3600 SIG NXT 5 2 3600 20030510221048 (
20030410221048 56954 freeswan.nl.
[...] cNkca6K/mc9M32VD6gRp )
www.freeswan.nl. 3600 IN A 193.110.157.9
3600 SIG A 5 3 3600 20030510221048 (
20030410221048 56954 freeswan.nl.
fVXogRSsfmm5SStZ4rok )
3600 NXT freeswan.nl. A SIG NXT
3600 SIG NXT 5 3 3600 20030510221048 (
20030410221048 56954 freeswan.nl.
[...] bXLB4JYJx0fMWXehBYS7 )
```



Deploying DNSSEC

The Delegation problem

- _ The Parent should securely delegate authority of the child zone
 - _ Parent cannot give a "non-authoritative" answer
- _ Parent cannot not sign child zone data
 - _ It has no private key of child
- _ Parent should not sign child zone data
 - _ It is not authoritative for child zone
- _ Parent will need to serve NS (and perhaps glue) records of child zone
- _ Answer needs to be secure



Black Hat®

Europe 2003

Deploying DNSSEC

DNSSEC: The DS record

```
Rlabel TTL IN DS <key tag> <algorithm> <20 bit SHA-1 Digest>
```

```
reeswan.nl.      345600 IN NS ns.xtdnet.nl.
reeswan.nl.      345600 IN NS ns1.xtdnet.nl.
reeswan.nl.      345600 IN DS 49601 5 1 (
                    C7D3B76F7DEE10E6A73B7D0F6EDAF55FFF60CA78 )
reeswan.nl.      345600 IN SIG DS 1 2 345600 20030416070311 (
                    20030409070311 6869 nl.
```

```
V2pmK7IGF1W7SDJxxyTep707IDRQ36IEkmyEhezJO72U
3g1YeWTI4r5ISAOkGW/+u74FRuQgMFzYzRisCZKYCiBm
rNiatRg+TTf9+yzJcqg9A2CuygNbi8I7aVloYxsM+qri
9J1CJQuxAzbKLPAppQw4UP1VOiB4NvHWG2jwFNw= )
```

These are all reeswan.nl records at the parent



Black Hat®

Europe 2003

Deploying DNSSEC

Delegation fixed: chain of trust

- _ In an ideal world: Only one trusted key is needed
 - The root (".") key
- _ In the real world: Secure entry points
- _ Your world: Make your own trusted key(s)

```
trusted-keys {
  "nl." 256 3 1
  "AQOtBQXOH5L/wmOt01PuxXAfSk1bw/dneW
  PoCyl4yi8tLCjz+DkAs0mz AAvd9XUNp
  YDaf5KTciSs9254oeiE0s0FuYbxS4nm7
  veZSPCgWoHULFNJ tKPNeb4EEbINkAsE
  GagwQJoIrjIAYKx4CEn3hPwEIUIVko23
  I5tSSPPs sxrVnQ==";
}
```



Black Hat®

Europe 2003

Deploying DNSSEC

Problem: Time is not on our side

- _ Small keys can be attacked using brute force
- _ Large keys are strong, but CPU expensive
- _ Keys can become useless
 - _ Key can be stolen, lost or compromised
 - _ Key can be based on impure random
 - _ Key can leak information when in use (DSA)
- _ Keys will need to be replaced at some point
 - _ Parent needs to be (securely) informed to update DS record
 - _ We want to minimize parent <-> child interaction
 - _ Cache, TTL, Signature expiration: Both keys are needed at the same time



Black Hat®

Europe 2003

Deploying DNSSEC

Two keys: ZSK and KSK

One Zone Signing Key (ZSK, 768bit, one month)

- 768bit
- Validity of one month
- Signs all Rrsets in the zone (including KEY records)
- Can be changed without parent notification

One Key Signing Key (KSK, 2048bit, one year)

- Parent's DS record points to this key
- 2048bit
- Validity of one year
- Only signs the key records
- Must inform parent when this key changes



Deploying DNSSEC

Scheduled ZSK Rollover

	normal	prepare	
rollover			
parent:	DS(KSK)	DS(KSK)	
DS(KSK)			
child:	KSK	KSK	KSK
	ZSK1	ZSK1, ZSK2	
	ZSK2		
	KSK(KSK,ZSK1)	KSK(KSK,ZSK1,ZSK2)	
	KSK(KSK,ZSK2)		
	ZSK1(zone)	ZSK1(zone)	
	ZSK2(zone)	ZSK2(zone)	
	ZSK2(zone)		



Deploying DNSSEC

Scheduled KSK Rollover

	normal	prepare	rollover
parent:	DS(KSK1) DS(KSK1)		DS(KSK2)
child:	KSK1	KSK1, KSK2	
	ZSK	ZSK	
	ZSK		
	KSK1(KSK1, ZSK)	KSK1(KSK1, KSK2, ZSK)	
	KSK2(KSK2, ZSK)		
	ZSK(zone)	ZSK(zone)	
	ZSK(zone)	ZSK(zone)	
	ZSK(zone)	ZSK(zone)	



Black Hat®

Europe 2003

Deploying DNSSEC

Unscheduled Rollover

PANIC!!!

- Have emergency procedure ready!
- Have spare KSK in zone for emergency rollover?
- Contact everyone who has your key as trusted key
- Contact children
- Short TTL's and short SIG lifetime help contain disaster
- Emergency out of bound contact needed with parent

ZOR1(ZONE)

ZOR1(ZONE)

ZOR2(ZONE)



Deploying DNSSEC

Setup bind

- _ Only use latest snapshot on signer machine
 - As of writing: bind-9.3.0s20021217
 - ./configure --with-openssl
 - Threads broken in latest snapshot, use --disable-threads
- _ Do not use "host" or "nslookup"
 - For "host" like output, use "dig +multiline"
 - For dnssec, use "dig +dnssec"
 - To ask for data without checks, use "dig +cdflag"
- _ You can use stable bind8/9 to serve secure zones
 - Note: bind8 does NOT serve data with expired SIG record. This data will disappear on bind8. Bind9 serves data with expired SIG records



Black Hat®

Europe 2003

Deploying DNSSEC

Bind: Create secure zonefile

```
~> dnssec-keygen -a RSASHA1 -b 2048 -n ZONE freeswan.nl  
Kfreeswan.nl.+005+49601
```

```
~> dnssec-keygen -a RSASHA1 -b 768 -n ZONE freeswan.nl  
Kfreeswan.nl.+005+56954  
(creates .key and .private files)
```

```
~> cat *key >> /var/named/freeswan.nl  
(increase serial number in zone)
```

```
~> dnssec-signzone -o freeswan.nl -k Kfreeswan.nl.+005+49601.key  
/var/named/freeswan.nl Kfreeswan.nl.+005+56954.key
```

(upload to master and change named.conf to load zone "freeswan.nl.signed" instead of "freeswan.nl")

```
Test: dig +multiline +dnssec +key freeswan.nl @ns.vtdnet.nl
```




Black Hat®

Europe 2003

Deploying DNSSEC

Secure .nl: <http://secreg.nlnetlabs.nl/>

File Edit View Go Bookmarks Tools Help

http://secreg.nlnetlabs.nl/cgi-bin

Linux

SECREG: .NL

make secure | block | key rollover | change secc | whois notify
tools | zone listing | forms | procedures | about

Make a .nl domain secure

Zone key(s) from fnl.nl

Please select the KEY you want to use as your zone KEY

```
fnl.nl. 3600 IN KEY 256 3 5 (
AQPAUnFSM/w9du2kBlASmFseQmuUPeIQ/tVf
Op2wT8WwOkx9kH8hm0/Of3YNU1FZ+gtIkx7
qlkpvYq6mYZuvLXBgFFU4IqwAU12C4kdayg
Jrt3/roq2h5rbTBcCooWMeHSIr6uL1N1RXPg
/pet17jRXPgXQKfeAzQsIUUUi4gFdw==
) ; Key ID = 25541
```

```
fnl.nl. 3600 IN KEY 256 3 5 (
AQO5rfR72fQkQFVn1kvYwhMPMmstyumSSCwU
PEA6dFN4asz8uo9B1wlbXEJKEsWCsAwYctBr
C6fzRxVItJ9spmlUcD/W2vMsOp9oIFJxOVRp
sw5qVugdPdRna2n4oPPZ9PBvNjinLNFoBJnt
GLZLeZ3HrQ3d5nryrHO1EEabaD4Esw==
) ; Key ID = 16217
```

Proceed Clear



Black Hat®

Europe 2003

Deploying DNSSEC

Secure .nl: <http://secreg.nlnetlabs.nl/>

The screenshot shows a web browser window with the address bar containing `http://secreg.nlnetlabs.nl/cgi-bin/`. The page title is "SECREG: .NL". The main content area has a green header with navigation links: "make secure | block | key rollover | change secc | whois notify" and "tools | zone listing | forms | procedures | about". Below this is a section titled "Key rollover" with a form. The "Domain name:" field contains "ct.nl". Under "Authentication", the "Sign this record:" field contains "3600 IN TXT \"random txt m8OfNOLtmpXz2aQ\"". Below this, it says "use [sign.pl](#)". A large text area contains the following DNS record output:

```
ct.nl. 3600 IN SIG TXT 5 2 3600 20030315125047 (
20030213125047 35861 ct.nl
KHR718ehTtidLkTUbnf+NPPJynSo2jvrVikP0vjKysPTe
v6tRocPkV02p2xnn7aR3h0CrMAVnva7WCUJ4GsdPJD2fx
N0zYkH722evhVnasy5TTg0Q81cpVnbag/95/OR )
```

Below the text area are "Proceed" and "Clear" buttons. At the bottom left is the "NetLABS" logo.



Black Hat®

Europe 2003

Deploying DNSSEC

Securely Resolving .nl domains

Use bakbeest.sidn.nl or alpha.nlnetlabs.nl

```
;<<> DiG 9.3.0s20021217 <<> +dnssec +multiline -t a www.fnl.nl @bakbeest.sidn.nl
;; global options: printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 16017
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

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

;; ANSWER SECTION:
www.fnl.nl.          2998 IN A 193.110.157.9
www.fnl.nl.          2998 IN SIG A 5 3 3600 20030318164405 (
                    20030216164405 25541 fnl.nl.
                    gkMbAoyANPDh+3A71C7T1x2kApSax9gni/NJ2REbmUm0
                    qeZ6rTmePn+45qc6HdIvRitoUKiuyEHfBq5M9ilqoZ76
                    ASiCiXBqVJcvXvayKUDZJd7v6YN6Swc0i1RJMNaziBiG
                    wCWUDmCr4keujIe1SQFL5ZB3feVba7sv9KM1ueM= )

;; Query time: 50 msec
;; SERVER: 193.176.144.170#53(bakbeest.sidn.nl)
;; WHEN: Wed Feb 19 00:55:42 2003
;; MSG SIZE rcvd: 221
```



Black Hat®

Europe 2003

Deploying DNSSEC

DNSSEC for com/net/org domains

See: www.dnssec.verisignlabs.com

- No personal experience yet (sorry)
- Still needs pre-DS dnssec-makekeyset tool which is no longer in the bind snapshot (java signer available)
- Trusted keys need to be pulled from zonedata



Black Hat®

Europe 2003

Deploying DNSSEC

Deployment of many secure zones

_ Net::DNS and Net:DNS::SEC (in CPAN)

- Has bug for large TXT records (opportunistic encryption records)

_ DNSSEC-Maint and DNSSEC-Maint-Zone (RIPE)

- See blackhat CD
- Supports notion of KSK and ZSK
- Very easy to use and maintain keys, zones and rollovers (!)

- . Shell> create RSASHA1 zonesigning 768 freeswan.nl

- . Shell> dnssigner -o freeswan.nl /var/named/freeswan.nl

_ You can use stable bind8/9 to serve secure zones

- Note: bind8 does NOT serve data with expired SIG record. This data will disappear on bind8. Bind9 serves data with expired SIG records.



Black Hat®

Europe 2003

Deploying DNSSEC

Changes in organisation

- _ Location of DNS Zonefile now on secure signer machine
- _ New task: maintain secure zones
 - Don't let the SIG records expire!!
- _ No more direct edits of zonefile
 - Or extra step if generating from database (and how secure is the database machine?)



Black Hat®

Europe 2003

Deploying DNSSEC

Applications using DNSSEC

- _ FreeS/WAN: Ipsec opportunistic encryption
 - _ In development
- _ OpenSSH: host keys in DNS
 - _ Only patch for old version currently available
- _ ISC dhclient: secure dynamic updates
- _ NXT-walk software (tsk tsk)

- _ Browser plugins???



Black Hat®

Europe 2003

Deploying DNSSEC

DNSSEC References

- _ Bleeding edge: <http://www.ripe.net/dis/>
- _ Documentation:
 - _ <http://www.xtdnet.nl/paul/blackhat/> (updates of these slides)
 - _ <http://www.xtdnet.nl/paul/dnssec/>
 - _ <http://www.ripe.net/training/dnssec/>
 - _ <http://www.dnssec.nl/>
- _ Software
 - _ <ftp://ftp.isc.org/isc/bind9/snapshots/>
 - _ <http://www.miek.nl/projects/resolver/resolver.html>
- _ Secure register experiments
 - _ <http://secreg.ninetlabs.nl/>



Black Hat®

Europe 2003

Deploying DNSSEC

My ultimate goal:

Linux FreeS/WAN



_ Opportunistic Encryption: Ipsec for the masses

http://www.freeswan.org/freeswan_snaps/CURRENT-SNAP/doc/quickstart.html