DNSSEC, wat is het? Komt het er *ooit* nog van?

Miek Gieben
miek@{miek.nl,ATComputing.nl}

ATComputing, Nijmegen

NL Linux Gebruikers Groep, 7 juni 2008

1. Introductie

2. DNS
   - Globale architectuur
   - Basis begrippen
   - Zwakheden
   - Verbeteringen zonder DNSSEC

3. DNSSEC
   - Requirements voor DNSSEC
   - Public key cryptography
   - RFC4033/4034/4035
   - Verificatie
   - Chain of Trust
   - Implementatie
   - Deployment; uitrol

Wie

Miek Gieben

- betrokken geweest bij totstandkoming van RFC4033,34,35
- afgestudeerd op DNSSEC
- mede-auteur van RFC4641 - DNSSEC best current practices
- ldns - DNS(SEC) library àla Perl's Net::DNS maar dan in C
- NSD release manager, schreef `zone-compiler` (lexx/yacc)

Architectuur

DNS

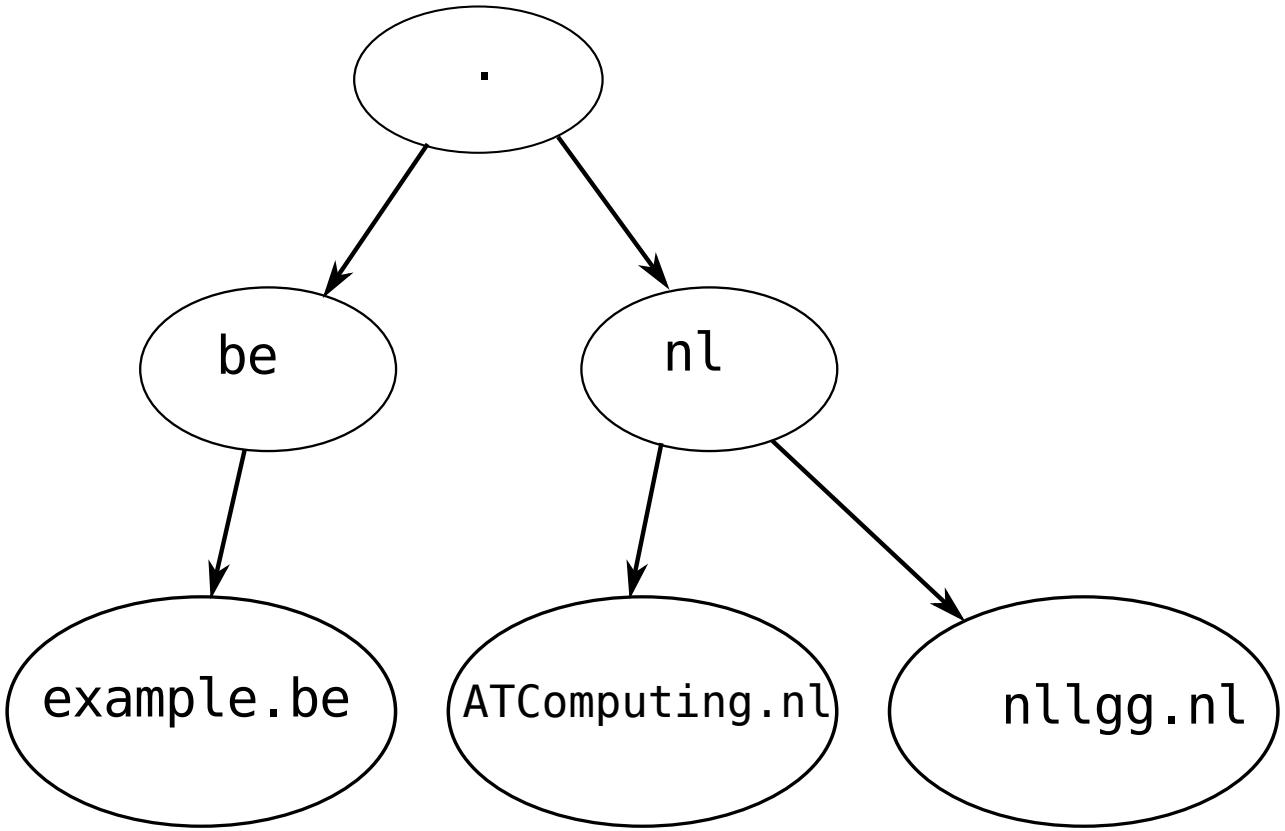
- heeft een boom structuur
- bovenin de root
- knooppunten zijn domeinen (nameservers)
- "kinderen" van knooppunten zijn gedelegeerde domeinen

DNS geeft antwoord op existentiële vragen, zoals

- wat is de mailhost van dit domein?
- wat je het IP adres van deze naam?
- wat is de naam van dit IP adres?
- bestaat deze naam? (`NXDOMAIN` antwoorden)

Geen database functionaliteit! (`SELECT mie* FROM .nl`)

De DNS boom



Begrippen

client/resolver draait lokaal, stelt voor jou vragen aan DNS

nameserver draait ergens op internet, geeft antwoord

cache lokaal of op internet, onthoudt antwoorden

De communicatie tussen al deze systemen kan verstoord worden door een aanvaller.

resource records kleinste stukje informatie binnen DNS

pakket bundeltje resource records

domeinen informatie over een stuk DNS; bestaat uit resource records

Zwakheden

man in the middle stuur een *fake* antwoord naar de client. Ben je eerder dan het *officiële* antwoord, dan heb je gewonnen

cache poisoning krijg het voor elkaar dat er in een cache informatie komt die niet juist is

gebruik van UDP juist bij UDP is het makkelijk om te *spoofen*

Het probleem van DNS: geen vertrouwen tussen client en server
op geen enkele manier vast te stellen of een antwoord goed is of dat er mee gerommeld is

DNS pakket

```
dig A www.atcomputing.nl

;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 43431
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ...

;; QUESTION SECTION:
;www.atcomputing.nl. IN A
;; ANSWER SECTION:
www.atcomputing.nl. 300 IN A 195.108.229.28
;; AUTHORITY SECTION:
atcomputing.nl. 798 IN NS ns.atcomputing.nl.
atcomputing.nl. 798 IN NS servix.tunix.nl.

;; Query time: 20 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Mon May 12 15:54:31 2008
;; MSG SIZE rcvd: 96
```

Aanvallen

. . . zijn geen bangmakerij, maar bestaan *echt*

```
% apt-cache show dsniff
Package: dsniff
Priority: extra
Section: universe/net
⋮
Description: Various tools to sniff network traffic for
cleartext insecurities.
This package contains several tools to listen to and create
network traffic.
Please do not abuse this software.
```

En ook

`http://packetstormsecurity.org/groups/ADM/ADM-DNS-SPOOF/`

Verbeteringen

Het *was* vrij gemakkelijk om DNS te spoofen

- query id *plus* UDP port randomizen
- caches moeilijker te vervuilen, nemen niet alles gewoon voor waar meer aan
- aanvaller heeft eigenlijk toegang tot netwerk kabel nodig
- . . . maar tegenwoordig veel wireless

Wat dan?

Aangenomen dat iets àla DNSSEC nodig is om het DNS te beschermen, hoe ziet dat eruit?

- geen state tussen server en client mogelijk, zoals SSL; rootservers kunnen dat niet aan
- geen on *the fly crypto*; root servers kunnen dat ook niet aan, ook ccTLD servers krijgen dan problemen
- liefst geen TCP

Wat dan?

We hebben dus iets nodig dat

- offline moet werken; client/server communicatie blijft het zelfde
- controle mogelijk of antwoord van juiste server komt
- controle mogelijk of antwoord onderweg niet veranderd is
- moeten mogelijk zijn om te zeggen dat iets niet bestaat

De gekozen oplossing:
Voeg *public key cryptography* toe aan het DNS

begrippen

public key crypto

Sleutel bestaat uit **geheim** (*private*) en **publiek** (*public*) deel. Geheime deel geheimhouden. Publieke sleutel verbinden met jouw digitale identiteit. Voorbeeld: PGP

coderen	verhaspel met publieke sleutel, alleen te lezen met geheime sleutel
signeren	verhaspel met geheime sleutel, controleer met publieke sleutel

DNSSEC gebruikt *signeren*: digitale handtekeningen

Opbouw

- elk domein krijg een sleutel en elk mogelijk antwoord krijgt een handtekening (`NXDOMAIN` - buiten beschouwing)
- publieke sleutel komt in een `DNSKEY` record
- handtekeningen worden off-line gemaakt en *daarna* in het DNS geplaatst
- elk record krijg een handtekening, komt in het DNS als `RRSIG` record

Dus, om een domein DNSSEC waardig te maken, moet je

1. sleutel paar maken (`dnssec-keygen`)
2. publieke sleutel aan je domein toevoegen (`vi`)
3. domein ondertekenen (`dnssec-signzone`)
4. resultaat in je nameserver zetten

Huidige DNS

Vergelijk DNSSEC operatie met huidige DNS operatie:

1. resultaat in je nameserver zetten

Ook hier: DNSSEC kost operationeel veel meer inspanning. `cron` is je vriend (maar niet je redder).

Antwoord verificatie

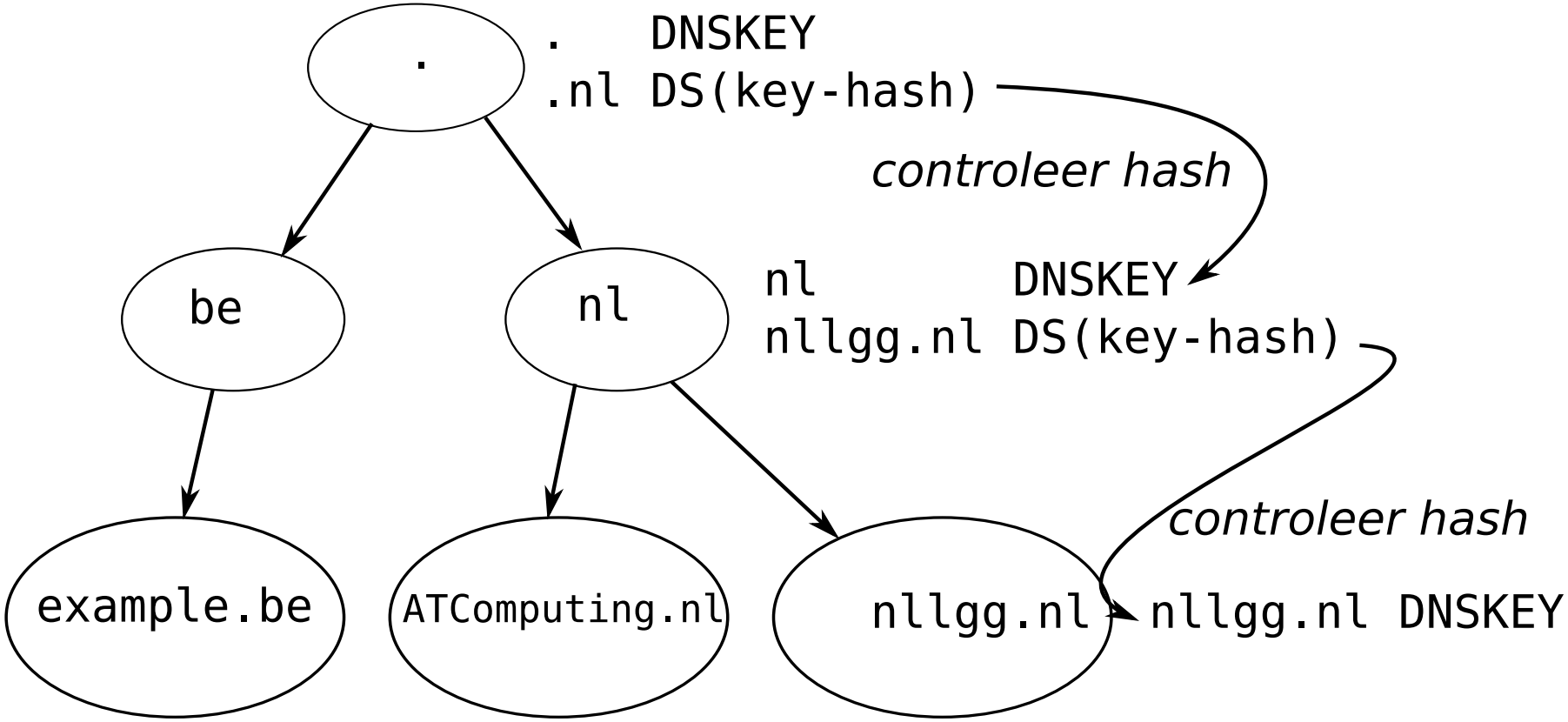
Stel je hebt de publieke sleutel van het domein in kwestie in handen...

1. vraag je vraag
2. wacht op het antwoord, *met* digitale handtekening
3. geen handtekening? $\longrightarrow$ gooi antwoord weg
4. wel handtekening, controleer de handtekening met de sleutel
5. handtekening niet correct $\longrightarrow$ gooi antwoord weg
6. handtekening wel correct? $\longrightarrow$ gebruik antwoord

Problemen

1. 100 miljoen domeinen, 100 miljoen sleutels...?
2. grote antwoorden, past dat nog wel in UDP pakketten?
3. uitrol nieuwe sleutels, hoe?

Follow the DS



- Elke DS wordt gevolgd *en* cryptografisch gechecked.
- `. DNSKEY` is de start (*secure entry point*).

Secure entry point

- Alleen de root key is nodig of een paar andere sleutels die hoog in de boom leven. Hiermee kun je de DS-en volgen en de sleutels van andere zones verkrijgen en controleren.
- Alleen van *die* eerste sleutel moet je zeker weten dat hij bij de root zone hoort.
- Daarmee is dus een veilig DNS gerealiseerd. . .

Hoe maak je zo'n sleutel en hoe ziet dat eruit?

```
dnssec-keygen -a RSASHA1 -b 1024 -n ZONE miek.nl
Kmiek.nl.+005+04830.key

miek.nl. IN DNSKEY 256 3 5 (
AwEAAa9LdCmFUNxB7Z9psHq/1lwFITStQuiatQuK/dFNCOMHfXmmzY/4
IJj6RkFGVzmCa8OUUhHvK947xN64bQmmuTjjUb7PFahqBkqQGOn/AcIp
KBPqOoDonkL46f4fSBenlMblbKMEdItj7QDde9jckkRtlGAiNsRD2DH+
Psn3RwvH )
```

`Kmiek.nl.+005+04830.private` bevat private key. Veilig bewaren!
Met deze private key daarna de zone signeren.

zone signing

```
dnssec-signzone -o miek.nl db.miek.nl Kmiek.nl.+005+04830.key
```

```
ls -l db.miek.nl*
-rw-r--r-- 1 miekg miekg 874 Jun 5 21:18 db.miek.nl
-rw-rw-r-- 1 miekg miekg 6942 Jun 5 21:18 db.miek.nl.signed
```

Nu klaar om in je nameserver te zetten.

DNSSEC pakket

```
dig A +dnssec www.nlnetlabs.nl

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 4096
;; ANSWER SECTION:
www.nlnetlabs.nl. 584 IN A 213.154.224.1
www.nlnetlabs.nl. 584 IN RRSIG A 5 3 600 20080629005005 (
20080601005005 18182 nlnetlabs.nl. V6593d8yXUrBq29zeAczv tDBJIl6wmcl

;; AUTHORITY SECTION:
nlnetlabs.nl. 2232 IN NS open.nlnetlabs.nl.
nlnetlabs.nl. 2232 IN NS ns7.domain-registry.nl.
nlnetlabs.nl. 2232 IN NS omval.tednet.nl.
nlnetlabs.nl. 10184 IN RRSIG NS 5 2 10200 20080629005004 (
20080601005004 18182 nlnetlabs.nl. nc8wOzecko ...+6lbUbI ynhI+dSjRW
SYo=)
;; ADDITIONAL SECTION:
...;; MSG SIZE rcvd: 973
```

Hele packet

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

;; ANSWER SECTION:
www.nlnetlabs.nl. 584 IN A 213.154.224.1
www.nlnetlabs.nl. 584 IN RRSIG A 5 3 600 20080629005005 20080601005005 18182 nlnetlabs.nl. V6593d8yXUrBq29zeAcz
GUgPCBe1RnfnpNNXfQe/j6/rEj3pYybwKvXfMJIkAW/JUV4mtGJ2l2E6 tDBJIl6wmcLd+QsNiZIyx7U+Mlweac61z8gSSW08BeA19/l17aD1Yg
V64=

;; AUTHORITY SECTION:
nlnetlabs.nl. 2232 IN NS open.nlnetlabs.nl.
nlnetlabs.nl. 2232 IN NS ns7.domain-registry.nl.
nlnetlabs.nl. 2232 IN NS omval.tednet.nl.
nlnetlabs.nl. 10184 IN RRSIG NS 5 2 10200 20080629005004 20080601005004 18182 nlnetlabs.nl. nc8wOzeckoU8OR+WNNY
HHHt/G/ofINhYlJubyuJbsNgshmJ0OeaFlSY/FwuEXl6sn6J+zAMwwr6 esB+9zG4+/m77vPunThCZ78pOsIf/ynhI+dSjRWd/IwPty6YdEe7QI
SYo=

;; ADDITIONAL SECTION:
omval.tednet.nl. 17912 IN A 213.154.224.17
omval.tednet.nl. 17912 IN AAAA 2001:7b8:206:1:200:39ff:fe59:b187
omval.tednet.nl. 17912 IN AAAA 2001:7b8:206:1::17
open.nlnetlabs.nl. 584 IN A 213.154.224.1
open.nlnetlabs.nl. 584 IN AAAA 2001:7b8:206:1::1
open.nlnetlabs.nl. 584 IN AAAA 2001:7b8:206:1::53
open.nlnetlabs.nl. 584 IN RRSIG A 5 3 600 20080629005005 20080601005005 18182 nlnetlabs.nl. MPfnsEdm27sG/grDD7K
Xqh6InkAocE3c+H1ge4Xkrkhc8y2bhIssP//FDWaO5Hkub298a0PAN18 wK0XTF/+eKppT8TNo4xv+DhHV7RzqfcAFq6lsAwXqrNUBzixgbm64Y
aC0=
open.nlnetlabs.nl. 584 IN RRSIG AAAA 5 3 600 20080629005005 20080601005005 18182 nlnetlabs.nl. npv0xEBVYWOvYDM3
Dc/cBzQsfqtKVGwy1EF9gXjiIem2Ln2IwYFjhSfZ9PGaWsBARXdBMGji oJgwrTPGBTG9ROWkPRcpTlZ2r71VuFKlBvllJN5Tz3dC/HLNXlvcSD
MOo=
```

Onze andere problemen

UPD pakket grootte

opgerekt van 512 bytes, naar aantal kB, mogelijk probleem voor hele oude machines/routers, meestal niet.
Omschakelen naar TCP?

Sleutels updaten

automatische procedures zijn moeilijk, als root zijn sleutel verliest iedereen kwetsbaar. Er zijn ideeën, maar niks concreets.

Deployment

- aantal landen heeft DNSSEC ingevoerd; oa Zweden (.se)
- Nederland denkt erover na, ook met andere zaken bezig (ENUM)
- markt vraagt (nog) niet echt om DNSSEC

Stap 0 Besluiten dat je .nl secure wilt maken
Stap 1

- .nl sleutel maken
- sleutel aan iedereen geven
- plan om de .nl sleutel regelmatig te updaten
- plan om de .nl sleutel te updaten na verlies/diefstal
- .nl domein signeren

Stap 2

- subdomeinen in .nl secure maken (`DS RR` in .nl zetten)

Wij zijn nu bij stap 0

Komt het er nog van?

- langzame deployment push van (cc)TLDs
- eind gebruikers amper geïnteresseerd
- overheid wil DNSSEC verplicht stellen (Department of Homeland Security)
- `.org` gaat waarschijnlijk DNSSEC invoeren

Persoonlijke mening

DNSSEC is *too* much, *too* late

Links en vragen?

Software

- BIND9, ISC
- NSD2/3, NLnetLabs
- Unbound, NLnetLabs

- RFC40{33,34,35}, *de* DNSSEC documenten
- RFC4641, DNSSEC Operational Practices
- http://www.dnssec.net
- http://www.dnssec-deployment.org
- http://www.nlnetlabs.nl
- http://www.isc.org

gemaakt mbv: LaTeXbeamer, `vim`, `evince` en `inkscape`