D N S S E C in der Praxis

Werkzeuge

für Key Management und Zone Signing

DENIC Technisches Meeting
4. April 2006

Holger.Zuleger@hznet.de

DNSsec oder "Wie signiert man eine Zone"

- Alle grundlegenden Werkzeuge liefert BIND
  - Zum Erzeugen der Schlüssel: `dnssec-keygen`
  - Zum Signieren der Zone: `dnssec-signzone`
- Keine Policy Definition möglich
  - Schlüsselalgorithmen
  - Schlüssellängen
  - Nutzungsdauer
- Kein automatischer Schlüsseltausch
  Wie kommen die Schlüssel in die Zone?
- Kein automatisches re-signing
  Wer erhöht die Seriennummer?
- Kein „reloading“ der Zone

DNSsec in der Praxis (Bind-Tools)

- Erzeugen des Schlüsselmaterials
  - — Key signing key (KSK)

    ```
    $ dnssec-keygen -f KSK -n ZONE -a DSA -b 1024 example.net
    ```

  - — Zone signing key (ZSK)

    ```
    $ dnssec-keygen -n ZONE -a RSASHA1 -b 512 example.net
    ```

```
$ ls -l
-rw-r--r--   1 dnsop  dnsop   581 2005-08-14 13:55 Kexample.net.+003+18710.key
-rw-------   1 dnsop  dnsop   688 2005-08-14 13:55 Kexample.net.+003+18710.private
-rw-r--r--   1 dnsop  dnsop   121 2005-08-14 13:55 Kexample.net.+005+57705.key
-rw-------   1 dnsop  dnsop   545 2005-08-14 13:55 Kexample.net.+005+57705.private
```

- Der öffentliche Teil der Schlüssel muß in die Zone

  ```
  $ cat Kexample.net+*.key >> zone.db
  ```

- Erhöhen der Seriennummer im SOA-Record (vi?)
- Signieren der Zonendatei

  ```
  $ dnssec-signzone -g -o example.net zone.db
  zone.db.signed
  ```

DNSsec in der Praxis (2)

- Bind konfigurieren

```
options {
    dnssec-enable yes;
};

zone "example.net" {
    type master;   file "example.net./zone.db.signed";
};
```

- Laden der neuen Zonendatei

```
$ rndc reload example.net
```

- Achtung! Re-signing der Zone vor Ablauf der Signaturen!
  Seriennummer erhöhen!

- Das Schlüsselmaterial sollte regelmäßig gewechselt werden
  Es gibt zwei unterschiedliche Prozeduren für Key Rollover

Schlüsseltausch (Key Rollover)

- Draft „DNSsec Operational Practices“ definiert zwei Verfahren
- ZSK Rollover (pre-publish key)
  1. Generiere einen zweiten ZSK
  2. Publiziere beide Schlüssel; Nutze nur den alten zum Signieren
  3. Warte mindestens: propagation time + TTL des DNSKEY−RR
  4. Signiere mit neuem Schlüssel; Publiziere nach wie vor beide
  5. Warte mindestens: propagation time + max TTL der alten Zone
  6. Entferne den alten Schlüssel aus der Zone
- KSK Rollover (double signature)
  1. Generiere einen zweiten KSK
  2. Benutze beide Schlüssel zum Key Signing
  3. Sende den neuen DS−Record zum Parent
  4. Warte bis DS in der Parentzone ist + TTL des alten DS−RR
  5. Entferne den alten Schlüssel

DNSsec Werkzeuge

- KROd − Key Rollover Daemon (www.idsa.prd.fr/index.php?page=kro&lang=en)
  - Vollautomatischer ZSK Schlüsseltausch
  - Vollautomatischer KSK Schlüsseltausch
    inkl. Bekanntgabe des KSK beim Parent
  - C−Programm als Frontend zu den BIND tools
  - Projekt ist abgeschlossen

- DNSSEC Key Maintenance Tools (www.ripe.net/disi/code.html)
  - Referenzimplementierung zu: „DNSsec Operational Practices“
  - Benutzt sicheren Bereich zur Speicherung der privaten Schlüssel
  - Unterschiedliche Frontends für Schlüsseltausch und Zone Signing
  - Halbautomatischer KSK und ZSK Schlüsseltausch
    (double signature & pre-publish)
  - Perl basierend

DNSsec Tools (2)

- DNSsec Tools (www.dnssec-tools.org)
  - Zone Signing und Key Management Werkzeug
  - Perl basierter Wrapper um die BIND tools
  - Beinhaltet zusätzlich DNSsec Resolver Bibliotheken (Patch für Sendmail(spf), Mozilla und Thunderbird)

- Zone Key Tool (www.hznet.de/zkt/)
  - Automatischer ZSK Schlüsseltausch
  - Vollautomatisches Re-Signing der Zone
  - Rudimentärer „named.conf“ Parser
  - C basiertes Frontend zu den BIND tools
  - Basiert auf standard Bind-Konfiguration
  - Entwickelt für kleine bis mittlere Anzahl von Zonen

Zone Key Tool (ZKT)

- Zwei Programme für Schlüsselmanagement und zum Signieren

```
$ dnssec-zkt
$ dnssec-signer -N /etc/named.conf
```

- Einfache Konfigurationsdatei (Policyfile) (Auszug aus `dnssec.conf`)

```
#   zone specific timing values
ResignInterval: 3d      # (259200 seconds)
Sigvalidity:    30d     # (2592000 seconds)
Max_TTL:        6h      # (21600 seconds)
Propagation:    5m      # (300 seconds)

#   signing key parameters
KSK_lifetime:   0
KSK_algo:       DSA     # (Algorithm ID 3)
KSK_bits:       1024
ZSK_lifetime:   10d     # (864000 seconds)
ZSK_algo:       RSASHA1 # (Algorithm ID 5)
ZSK_bits:       512
```

- Vollautomatischer ZSK Schlüsseltausch (pre-publish key algorithm)
- Automatische Erhöhung der Seriennummer in der Zonendatei
  Unterstützt sequentielle Nummerierung und `YYYYmmDDxx` Format

ZKT − Konfigurationsbeispiel

- Anlegen eines separaten Verzeichnisses für jede Zone (Verzeichnisname == Domainname)

```
$ mkdir example.net.
$ cd example.net.
```

- Format der Zonendatei (Standardname: `zone.db`)

```
$  head -15 zone.db
$TTL 7200
;    Be sure that the serial number below is left
;    justified in a field of at least 10 spaces!!
;                 0123456789;
@    IN SOA   ns1.example.net. hostmaster.example.net.  (
                 63         ; Serial
                 43200    ; Refresh
                 1800     ; Retry
                 2W       ; Expire
                 7200 )   ; Minimum

          IN  NS  ns1.example.net.
          IN  NS  ns2.example.net.

$INCLUDE dnskey.db        ;include the DNSKEY records
     ...
```

ZKT − Konfigurationsbeispiel(2)

- Anlegen einer (leeren) Datei `zone.db.signed`

```
$ touch zone.db.signed
$ ls -l
-rw-r-----   1 dnsop  dnsop   916 2005-08-14 13:54 zone.db
-rw-r--r--   1 dnsop  dnsop     0 2005-08-14 13:55 zone.db.signed
```

- Signieren der Zone

```
$ dnssec-signer -v -o example.net.
parsing zone "example.net." in dir "."
        No active KSK found: generate new one
        No active ZSK found: generate new one
        Re-signing necessary: Modified keys
        Writing key file "./dnskey.db"
        Incrementing serial number (64) in file "./zone.db"
        Signing zone "example.net."
$ ls -l
-rw-r--r--   1 dnsop  dnsop   581 2005-08-14 13:55 Kexample.net.+003+18710.key
-rw-------   1 dnsop  dnsop   688 2005-08-14 13:55 Kexample.net.+003+18710.private
-rw-r--r--   1 dnsop  dnsop   121 2005-08-14 13:55 Kexample.net.+005+57705.key
-rw-------   1 dnsop  dnsop   545 2005-08-14 13:55 Kexample.net.+005+57705.private
-rw-r--r--   1 dnsop  dnsop  1136 2005-08-14 13:55 dnskey.db
-rw-r--r--   1 dnsop  dnsop    71 2005-08-14 13:55 dsset-example.net.
-rw-r--r--   1 dnsop  dnsop   702 2005-08-14 13:55 keyset-example.net.
-rw-r-----   1 dnsop  dnsop   916 2005-08-14 13:55 zone.db
-rw-r--r--   1 dnsop  dnsop  4080 2005-08-14 13:55 zone.db.signed
```

ZKT − Konfigurationsbeispiel(3)

- Zeige den aktuellen Status der Schlüssel an

```
$  dnssec-zkt -a .
Keyname              Tag Typ Sta Algorit Generation Time             Age
example.net.     18710 KSK act DSA     Aug 14 2005 13:55:24     13m42s
example.net.     57705 ZSK act RSASHA1 Aug 14 2005 13:55:24     13m42s
```

- Anpassen des Dateinamens in `named.conf`

```
zone "example.net." in {
        type master;
        file "example.net./zone.db.signed";
};
```

- Erzwinge ein re-signing und reload der Zone

```
$  dnssec-signer -r -f -v -N named.conf
parsing zone "example.net." in dir "./."
        Re-signing necessary: Option -f
        Writing key file "././dnskey.db"
        Incrementing serial number (65) in file "././zone.db"
        Signing zone "example.net."
        Reload zone "example.net."
```

- Kontrolle des Logfile `/var/log/named`

14-Aug-2005 14:34:43.198 general: info: zone example.net/IN: loaded serial 65 **(signed)**

ZKT − Konfigurationsbeispiel(4)

- Regelmäßiges neusignieren der Zone
  Aufruf von `dnssec-signer` mindestens einmal täglich
- `cron` is your friend

```
$ crontab -l
21  6 * * * /home/dnsop/dnssec-cron 2>&1 | logger -t dnssec-cron -p daemon.info
21 18 * * * /home/dnsop/dnssec-cron 2>&1 | logger -t dnssec-cron -p daemon.info
```

- Das `dnssec-cron` Script ist einfach

```
echo "current zone signing keys"
/home/dnsop/bin/dnssec-zkt -z
echo "dnssec re-signing process started"
/home/dnsop/bin/dnssec-signer -v -v -r -N /var/named/named.conf
```

- Erzeugen der `trusted-keys`-Section für die Resolver Konfiguration

```
$ dnssec-zkt -T -l example.net.
trusted-keys {
"example.net."   257 3 3 "CJEUcyN1ES5bAnBI4O+m7nLhbmTfxVtF31O4agNVe+6Hu8kZ8EKzm+/U
                         +qh2NXv6+UgowadnPlfHHwLzpfNP4aZXfXa2qog1P5dp7POUquW6zn25
                                    ...
                         Wdlf/F/2lJh2LF4bU616EyOeRichLvlBXn15nkkLr4usbPitr68DrVas
                         o6bci4LJlPJBkHVS/3MtBo0lSY3XvoiBJtgp" ; # key id = 18710
};
```

Zusammenfassung

- BIND-Tools bieten grundlegende Mittel zum Signieren einer Zone
- Zusätzliche Werkzeuge stehen bereit:
  - Für Schlüsselmanagement
  - Für Automatisierung des Signing Prozesses
- Erste signierte Zonen verfügbar
  - `.se`
  - Alle RIPE Reverse Zonen (`.in-addr.arpa`, `.ip6.arpa`)
  - Zur Zeit ca. 450 `.de`−Domains
- Was fehlt:
  - Standards, Prozesse und Tools für DS Registrierung
  - Secure Resolver (Einige Bibliotheken bereits in Entwicklung)
  - Werkzeuge zum Resolver Management (SEP−Verwaltung)
  - Mehr secure TLDs! (`.de`, `.arpa`, `.com`, `.net`, `.org`, `.eu`)

Referenzen

Olaf Kolkman, Ripe-NCC DISI
„DNSSEC Howto Version 1.5“
(*http://www.ripe.net/disi/dnssec_howto/dnssec_howto.pdf*)

Nominum
BIND v9 Administrator Reference Manual
(*http://www.nominum.org/content/documents/bind9arm.pdf*)

RFCs 4033 (DNS Security Introduction and Requirements)
4034 (Resource Records for the DNS Security Extentions)
4035 (Protocol Modifications for the DNS Security Extensions)

Drafts DNSSEC Operational Practices
draft-ietf-dnsop-dnssec-operational-practices-06.txt

Links http://www.dnssec.net
http://secspider.cs.ucla.edu/secspider/
http://www.iks-jena.de/leistungen/dnssec/
http://www.hznet.de/dns/dnssec-denic040929.pdf
http://www.hznet.de/zkt/

Fragen ?

Fragen ?

http://www.hznet.de/dns/dnssec-denic060404.pdf

Fragen ?

http://www.hznet.de/dns/dnssec-denic060404.pdf

Herzlichen Dank für die Aufmerksamkeit

CONTENTS