Софийски Университет
"Св. Климент Охридски"

DNSSEC – възможности за употреба в БИОМ и колаборативен подход

Веселин Колев, Николай Николов

Софийски Университет
"Св. Климент Охридски"

DNSSEC – кратко описание

DNSSEC е технология, която:

- **позволява електронно подписване на ресурсните записи в зоните на домейни, с използване на криптография с публичен ключ (RSA и DSA базирана, използването на елиптични криви е в проект);**

- **урежда съхраняването на извършените върху ресурсните записи електронни подписи под формата на допълнителни ресурсни записи в същата зона;**

- **дава възможност за проверка на извършените върху ресурсните записи електронни подписи от страна на рекурсивни/кеширащи сървъри за имена, с цел проверка на автентичност на записите.**

Особености на DNSSEC:

- **използва се криптография с публичен ключ без сертификатен модел – не се използват сертификати и мета информация за ключовете;**
- **няма стандартно протоколно заложен механизъм за нецентрализирано унаследяване на доверието по схемата на извършване и проверка на електронните подписи;**
- **електронните подписи са добавени ресурсни DNS записи, които удостоверяват другите такива;**
- **свързаните с DNSSEC пакети са с по-голяма от стандартната дължина за протокола DNS и се налага използването на EDNS(0);**

Проблеми пред DNSSEC:

- **все още слаба поддръжка от страна на сървърския и клиентски софтуер;**
- **слабо разбиране на механизма на действие на DNSSEC от разработчиците на софтуер и сървърските администратори;**
- **проблеми свързани с EDNS(0) и защитните стени (разработчиците на филтриращ софтуер не са предвидили DNS пакети с такава дължина);**
- **изкуствено създавани политически проблеми пред централизираното използване на DNSSEC (кой да подписва зоната “.”).**

Най-добрата отправна точка за навлизане в DNSSEC е портала

http://www.dnssec.net/

Софийски Университет
"Св. Климент Охридски"

DNSSEC – подписване на ресурсни записи в зона на домейн

(примери за BIND9)

Необходим инструментариум за електронно подписване (UNIX/Linux):

- **инсталиран пакет BIND9 (преп. версия по-висока от 9.2) с налични в него инструменти:**

- `dnssec-keygen`
- `dnssec-signzone`

- **генератор на случайни числа с голяма периодичност и висока степен на хомогенност:**

- `/dev/urandom`

Генериране на KSK (двойка за подписване на ключове):

```
$ dnssec-keygen -r /dev/urandom -a RSASHA1 -b 4096  \
-f KSK -n ZONE example.com
```

Параметри на генерираната двойка:

- **тип на двойката: KSK (за подписване на ключове)**
- **име на подписваната зона: example.com**
- **криптиращ/подписващ алгоритъм: RSA**
- **дължина на криптиращия ключ: 4096 бита**
- **хеш функция за подписване: SHA-1**
- **използван генератор на случайни числа: `/dev/urandom`**

Генериране на ZSK (двойка за подписване на ресурсни записи):

```
$ dnssec-keygen -r /dev/urandom -a RSASHA1 -b 1024  \
-n ZONE example.com
```

Параметри на генерираната двойка:

- **тип на двойката: ZSK (за подписване на ключове)**
- **име на подписваната зона: example.com**
- **криптиращ/подписващ алгоритъм: RSA**
- **дължина на криптиращия ключ: 1024 бита**
- **хеш функция за подписване: SHA-1**
- **използван генератор на случайни числа: `/dev/urandom`**

Примерни файлове съдържащи двойките:

- **за KSK двойката:**

```
Kexample.com.+005+22818.key
Kexample.com.+005+22818.private
```

- **за ZSK двойката:**

```
Kexample.com.+005+49399.key
Kexample.com.+005+49399.private
```

Общ шаблон за наименоване на файловете:

K<име на зона>+005+<случайно число до 2^16>.<тип на ключа>

- Прибавяне на публичните ключове на двойките във файла на зоната:

```
$include “Kexample.com.+005+22818.key”
$include “Kexample.com.+005+49399.key”
```

- Електронно подписване на всички ресурсни записи в зоната:

```
$ dnssec-signzone -r /dev/urandom \
    -k Kexample.com.+005+22818 \
    -o example.com example.com \
    Kexample.com.+005+49399
```

- Файл съдържащ подписаната зона (задава се за прочит от BIND9):

```
example.com.signed
```

Ръководство за DNSSEC подписване на зони на домейни на български език е достъпно на адрес:

http://www.vesselin.org/papers/xhtml/bind9-dnssec.html

Софийски Университет
"Св. Климент Охридски"

Сървърски софтуер за поддръжка на DNSSEC

Поддръжка на DNSSEC на ниво "authoritative server":

- **изисква се поддръжка на DNSSEC ресурсни записи в обслужваните зони на домейни (http://www.dnssec.net/rfc);**
- **двата най-популярни сървърски софтуера за реализиране на "authoritative" DNS сървър – BIND9 и PowerDNS поддържат DNSSEC.**

Поддръжка на DNSSEC на ниво рекурсивен/кеширащ сървър за имена за сега се предлага най-пълно от BIND9 (текуща подходяща за използване версия е 4.6.0-P1):

- **валидация на база локално инсталирани и читаеми от BIND публични KSK ключове;**
- **валидация на база DLV записи и DLV базиран корен (виж. dlv.isc.org);**
- **режим на задължителна валидация и отказ от обслужване на записи с невалиден електронен подпис.**

Софийски Университет
"Св. Климент Охридски"

Настройки на BIND9 за поддръжка на DNSSEC

“authoritative only”

- **DNSSEC поддръжка в BIND9 следва да се използва за версии 9.2.0 и по-високи;**

- **Обслужването на свързани с DNSSEC записи, се реализира чрез прибавянето на**

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

във файла `/etc/named.conf`.

Описание на подписана зона на домейн в named.conf

```
zone “example.com” {
    ...
    file “data/example.com.signed”;
    ...
};
```

Проблеми при обслужването на DNSSEC подписани зони в BIND9:

- **BIND9 не поддържа автоматично подписване на динамични зони на домейни (такива с описателна клауза “allow-update”);**
- **няма възможност за проверка на електронния подпис при трансфер (частично проблема се решава с TSIG подписване на трансфера).**

Софийски Университет
"Св. Климент Охридски"

Модели на транзитивно доверие в DNSSEC

Йерархичен модел на транзитивност на доверието в DNSSEC:

- **всеки дъщерен домейн се удостоверява от майчиния домейн;**
- **удостоверяването на дъщерния домейн става чрез публикуване на DS ресурсни записи за неговия KSK в зоната на майчиния домейн и подписването им;**
- **всеки домейн може да бъде дъщерен освен домейна “.” - той може да бъде само майчин.**

DLV модел на доверие в DNSSEC:

- **съществува зона на домейн, в която се публикуват DLV записи за KSK публичния ключ на даден домейн (напр. dlv.isc.org);**
- **рекурсивните/кеширащите сървъри за имена се настройват да запитват DLV зоната за извличане на DLV записи за домейн, група домейни или всички домейни в DNS;**
- **DLV допуска съществуването само на един майчин домейн (описан чрез DLV зоната) и всички останали домейни (регистрирани чрез майчиния) са дъщерни, без продължение на тази йерархия.**

Съпоставка на DLV и йерархичната схема на доверие в DNSSEC:

- **йерархичният модел е политически обременен (засега) – трябва да се реши кой да подписва зоната на домейна ".", но е скалируем и не зависи от общия брой DNSSEC делегирани домейни;**
- **DLV замества йерархичния модел, но не е скалируем, защото трябва в една зона да съберат записи за всички DNSSEC делегирани домейни (тежка или невъзможна задача);**
- **йерархичният модел би бил подчинен на доверието в ICANN, което се реализира на база на кореновите сървъри в DNS, докато за DLV източника на доверие не може да бъде формулиран ясно.**

Съпоставка на DLV и йерархичната схема на доверие в DNSSEC:

- **за да работи DNSSEC с йерархичния модел, се изисква всеки сървър за имена да има само копие от KSK публичния ключ на “.” зоната;**
- **DLV е решение за случаите на организационни мрежи с непублични DNS домейни, неорганизирани в ясна йерархия, които трябва да се удостоверяват само за вътрешни нужди през една DLV зона на домейн;**
- **йерархичният модел също може да се използва за вътрешни за организациите домейни, когато последните имат ясна йерархия.**

Частична йерархичност на DNSSEC (в очакване на подписването на “.”):

- **Някои ccTLD като .bg, .se и др, са върхове на йерархията на доверие в DNSSEC за своите дъщерни домейни и всеки рекурсивен/кеширащ сървър за имена, притежаващ копие на KSK на майчината зона, би могъл да валидира електронното подписване в дъщерните домейни на ccTLD, без копие от техния KSK ключ;**

- **RIR RIPE е връх на доверието в DNSSEC за всички in-addr.arpa и ip6.arpa майчини домейни, които оперира.**

По-важни проекти, реализиращи частична йерархичност или DLV:

- **Deployment of Internet Security Extensions (DISI) – RIPE:**

http://www.ripe.net/disi/

- **ISC's DLV Registry – Internet System Consortium:**

https://www.isc.org/solutions/dlv

Софийски Университет
"Св. Климент Охридски"

Настройки на BIND9 за поддръжка на DNSSEC

рекурсивен/кеширащ сървър с валидация

Общи указвания в секцията `options` на `named.conf`:

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

Указвания в секцията `options` на `named.conf` за използване на йерархията на проекта DISI на RIPE:

```
options {
        ...
        dnssec-enable yes;
        dnssec-validation yes;
        dnssec-must-be-secure * yes;
        ...
};
include “/etc/ripe-ncc-dnssec-keys-new.txt”;
```

Копие от KSK публичния ключ на Register.bg може да бъде получено така:

```
$ dig @ns.register.bg -t DNSKEY bg
```

а от отговора трябва да се извлече ключа с идентификатор на роля 257 (роля на KSK) и да се постави във файл, читаем от BIND9, който след това да се включи в секцията `trusted-keys` на `named.conf`. В секцията `options` трябва да се прибави (ако не е добавено):

```
dnssec-must-be-secure * yes;
```

Преди да се извърши прибавянето на ключа, следва да се уточни автентичността му посредством контакт с техническите лица на Register.bg.

Копие от KSK публичния ключ на dlv.isc.org може да бъде получено на адрес:

http://ftp.isc.org/www/dlv/dlv.isc.org.key

(да се провери прилежащия към този файл OpenPGP електронен подпис)

То трябва да се прикрепи в секцията `trusted-keys` на `named.conf`. В секцията `options` трябва да се прибави (ако не е добавено):

```
dnssec-must-be-secure * yes;
```

Софийски Университет
"Св. Климент Охридски"

DNSSEC делегиране на in-addr.arpa домейни през RIPE DB

Условия за DNSSEC делегиране на in-addr.arpa домейн през RIPE DB:

- `domain` обект в RIPE DB за съответния in-addr.arpa домейн;
- `mntner` обект с права за модификация на `domain` обекта;
- възможност за удостоверяване чрез правомощията на `mntner` обекта;
- генериран `DS` ресурсен запис, който се поставя в `domain` обекта (генерира се при използването на `dnssec-signzone` като допълнителен файл с ресурсни записи);
- познания за работа с обекти в RIPE DB;
- предварително подписана зона на домейна.

Шаблон за domain обекта в RIPE DB

```
domain:         96.44.62.in-addr.arpa
source:         RIPE
descr:          University of Sofia
mnt-by:         AS5421-MNT
ds-rdata:       2197 5 1 C83E36ADBC68044C3AB1C3157F4C219E0F61F792
nserver:        ns.uni-sofia.bg
nserver:        ady.uni-sofia.bg
changed:        vlk@lcpe.uni-sofia.bg 20060904
changed:        vlk@lcpe.uni-sofia.bg 20090112
changed:        vlk@lcpe.uni-sofia.bg 20090113
tech-c:         SD2427-RIPE
tech-c:         GN1498-RIPE
tech-c:         VK1242-RIPE
zone-c:         SD2427-RIPE
zone-c:         GN1498-RIPE
zone-c:         VK1242-RIPE
admin-c:        KS2437-RIPE
```

OpenPGP подписан шаблон за domain обекта в RIPE DB

```
-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA256

domain:         96.44.62.in-addr.arpa
...
mnt-by:         AS5421-MNT
ds-rdata:       2197 5 1 C83E36ADBC68044C3AB1C3157F4C219E0F61F792
nserver:        ns.uni-sofia.bg
nserver:        ady.uni-sofia.bg
...
admin-c:        KS2437-RIPE

-----BEGIN PGP SIGNATURE-----
Version: GnuPG v1.4.5 (GNU/Linux)

iQIVAwUBSWyiyWWCvwTlRKnVAQh47A/9FZbCPwCNIJBQs6ie5SE9D/hDHQUAoJmx
...
=Xogi
-----END PGP SIGNATURE-----
```

- **Принцип на добра практика е при актуализация на обекти (създаване/модифициране/изтриване), да се използва удостоверяване пред RIPE DB без социален фактор, т.е. да не се използва парола. Най-висока сигурност в момента се постига чрез комбинация от електронно подписване на шаблона с OpenPGP и изпращането му до RIPE DB през SSL криптиран канал. За повече подробности:**

  http://www.vesselin.org/papers/xhtml/ripedb-updates-openpgp-howto.html

- **Изпращането на OpenPGP подписани шаблони през некриптиран комуникационен канал е крайно опасно. За подробности:**

  http://www.vesselin.org/papers/xhtml/no-ticket-signing.html

Отговор от RIPE DB за успешна актуализация на domain обекта (1/2)

```
 - From-Host: 2a01:288:8001:1::3
 - Date/Time: Mon Jan 12 21:02:26 2009

SUMMARY OF UPDATE:

Number of objects found:                    1
Number of objects processed successfully:   1
  Create:                   0
  Modify:                   1
  Delete:                   0
  No Operation:             0
Number of objects processed with errors:    0
  Create:                   0
  Modify:                   0
  Delete:                   0
  Syntax Errors:            0


DETAILED EXPLANATION:
```

Отговор от RIPE DB за успешна актуализация на domain обекта (2/2)

```
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
The following object(s) were processed SUCCESSFULLY:

- ---
Modify SUCCEEDED: [domain] 96.44.62.in-addr.arpa

***Info: Authorisation for existing [domain] 96.44.62.in-addr.arpa
         using mnt-by:
         authenticated by: AS5421-MNT

***Info: Parent has RIPE NCC nameservers.

***Info: RDNS Authorisation passed

***Info: Authorisation for  [domain] 96.44.62.in-addr.arpa
         using mnt-by:
         authenticated by: AS5421-MNT

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
```

Проверка за успешност на актуализацията на шаблона за domain обекта в RIPE DB

```
$ whois3 -B 96.44.62.in-addr.arpa

...

domain:         96.44.62.in-addr.arpa
mnt-lower:      AS5421-MNT
source:         RIPE # Filtered
descr:          University of Sofia
mnt-by:         AS5421-MNT
ds-rdata:       2197 5 1 C83E36ADBC68044C3AB1C3157F4C219E0F61F792
nserver:        ns.uni-sofia.bg
nserver:        ady.uni-sofia.bg
tech-c:         SD2427-RIPE
tech-c:         GN1498-RIPE
tech-c:         VK1242-RIPE
zone-c:         SD2427-RIPE
zone-c:         GN1498-RIPE
zone-c:         VK1242-RIPE
admin-c:        KS2437-RIPE
```

Софийски Университет
"Св. Климент Охридски"

DNSSEC делегиране на домейн в TLD BG

Условия за DNSSEC делегиране на домейн в TLD BG:

- **регистриран от Register.bg домейн в TLD BG;**
- **X.509 сертификат за универсален електронен подпис издаден от някои от удостоверителите по ЗЕПЕД;**
- **права за управление на информацията за домейна в портала http://www.register.bg;**
- **генериран `DS` ресурсен запис, който се поставя в описанието на домейна;**
- **предварително подписана зона на домейна.**

Проверка на DNSSEC делегирането чрез whois услугата на Register.bg (1/2)

```
$ whois3 -h whois.register.bg uni-sofia.bg

DOMAIN NAME: uni-sofia.bg
requested on: 12/12/1994 00:00:00 EET
processed from: 12/12/1994 00:00:00 EET
activated on: 15/12/1994 00:00:00 EET
expires at: 01/01/2011 00:00:00 EET
registration status: Registered

REGISTRANT:
Sofia University
  gr.SOFIA, 1504
  BULGARIA
...

DNSSEC: Active
```

Проверката на DNSSEC делегирането е възможна и през формата за справки на адрес:

https://www.register/bg

(от менюто в ляво се избира “Справки”).

Информацията за статуса на DNSSEC делегирането се предоставя по подразбиране за всеки регистриран от Register.bg домейн, без значение дали за него има или няма делегиращи записи (DS).

```
$ dig +dnssec +multiline @ns.register.bg -t ds uni-sofia.bg

...

;; ANSWER SECTION:
uni-sofia.bg.           345600 IN DS 43438 5 2 (
                                556387248B1CFD5D7556C0801CBAF26A2F53C27404B7
                                82C628D4D3BE2D15045D )
uni-sofia.bg.           345600 IN RRSIG DS 5 2 345600 20090212180005 (
                                20090113180005 59778 bg.
                                0G7MN64WToFGwyLGau+IqByg9H0u+bp6XyJM8pCKPod4
                                /RYlq8mvFNjC8foMQchwZCyZzro5nfl4TRy4sFXi/wfd
                                yoTzU/f2Vemq0tfVrvOkRDgwHnshql7u85Lr2SlM/KXH
                                bLo2wULd9sy6mqKvH59unIelzARM8BbTGrZhqZ8= )
```

Софийски Университет
"Св. Климент Охридски"

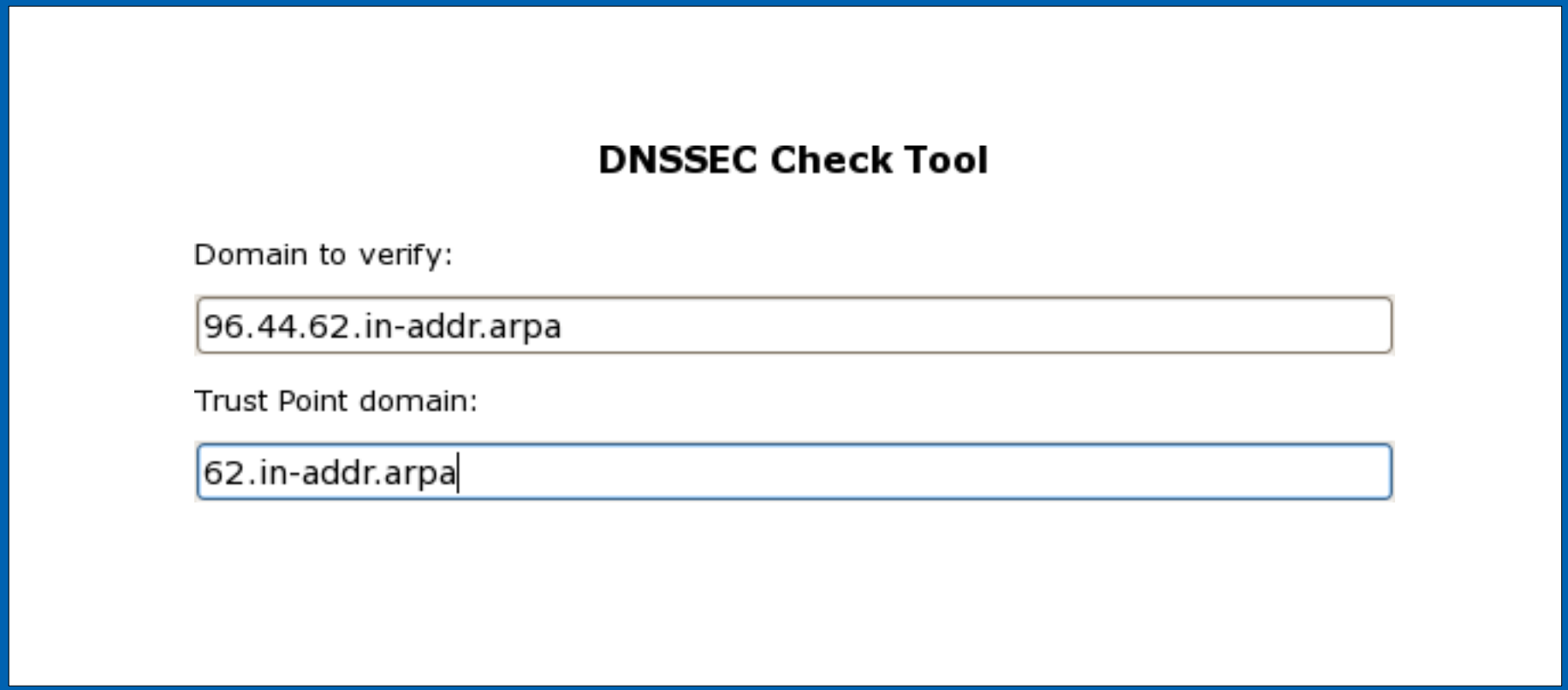
Публично достъпни инструменти за проверка на DNSSEC делегирането

Проект: ***"DNSSEC Trial México"***

http://www.dnssec.org.mx/

- **Колаборативен проект в обществена полза между NIC Mexico и Tecnológico de Monterrey Campus Monterrey;**
- **Предоставя уеб базиран интерфейс за проверка на DNSSEC делегирането;**
- **Предоставя възможност за въвеждане на публичния KSK с цел проверка на делегирането в "остров" на доверие;**
- **Интерфейсът има възможност за изследване на йерархията на унаследяване на доверие в DNSSEC:**

http://www.dnssec.org.mx/checkdnssec.html



Проект: *"SecSpider the DNSSEC Monitoring Project"*

http://secspider.cs.ucla.edu/

- Проектът работи в обществена полза и е колаборация между университети в САЩ (Калифорнийски университет, Университет на Колорадо);
- Извършва анализ на DNSSEC параметрите и правилността на делегиране за зоните на домейни, прибавени в базата данни на проекта - прибавянето на DNSSEC делегирана зона в базата на проекта е свободно и става през уеб базиран интерфейс;
- Изследва "островите" на доверие в DNSSEC;
- Предоставя публично достъпна статистика за броя регистрирани зони в проекта, параметрите им (например статистика за времето на живот на използваните ключове) и др. полезна информация.

Софийски Университет
"Св. Климент Охридски"

Ротация на ключовете в DNSSEC

Що е то ротация на ключове в DNSSEC:

- всяка двойка ключове използвана в криптографията с публичен ключ има срок на употреба, зависещ от няколко фактора (най-вече от вероятността за разкриваемост на частния ключ по известен публичен);
- нужна е периодична подмяна на KSK и ZSK двойките, за да се избегне повишаването на вероятността за разкриване на подписващия (частния) ключ;
- ротацията на ключовете в DNSSEC е действие за подмяна на използваните двойки ключове с нови, без при това да се препятства валидацията;
- ZSK подписващия ключ е с по-малка дължина и ротацията на ZSK е по-честа от тази на KSK.

Принципи за извършване на ротацията:

- **ZSK двойка с дължина на подписващия (частния) ключ от 1024 бита следва да се ротира на всеки 2 месеца (параноя);**
- **ZSK двойка с дължина на подписващия (частния) ключ от 2048 бита следва да се ротира на всеки 12 месеца (параноя);**
- **KSK двойка с дължина на подписващия (частния) ключ от 4096 бита следва да се ротира на всеки 5-7 години (параноя);**
- **ротацията на ZSK се изършва в зоната на домейна, а тази на KSK се извършва най-често в регистъра на домейна и не бива да е честа.**

Техника на ротацията на ZSK:

- публичният ключ на новата ZSK двойка се поставя като DNSKEY запис успоредно със стария;
- изчакват се TTL секунди (тези за стария DNSKEY запис) и едва след това зоната се преподписва с подписващия (частния) ключ на новата двойка и в новата си версия се подава на BIND за прочит;
- след изтичане на TTL секунди (отчетени по записа в зоната с най-голям TTL), след прочита от страна на BIND на преподписаната зона, се премахва DNSKEY записа за публичния ключ на старата ZSK двойка и зоната се преподписва;
- старият подписващ (частен) ключ и всички негови копия се унищожават (!)

Техника на ротацията на KSK:

- публичният ключ на новата KSK двойка се поставя като DNSKEY запис (успоредно със стария) и се генерират новите DS ресурсни записи; зоната се преподписва с текущия ZSK частен ключ и новата ѝ версия се подава за прочит на BIND;

- новите DS ресурсни записи се поставят в майчината зона, а старите се премахват;

- DNSKEY записа за старата KSK двойка се премахва след TTL(стар DS) +TTL(стар DNSKEY) секунди - началото на отчитане на периода е след синхронизацията на промените в майчината зона (отчитащи новите DS записи); старият подписващ (частен) KSK ключ се унищожава (!)

Инструментариум за автоматична ротация:

Проект “DNSSEC Tools”

http://www.dnssec-tools.org/

Софийски Университет
"Св. Климент Охридски"

Някои аспекти на сигурността в DNSSEC

Сигурност при работа с DNSSEC ключове:

- **генерирането на частни ключове следва да се извършва върху сигурни системи, с подходящ дългопериодичен генератор на случайни числа, с разпределение близо до хомогенното (напр. /dev/urandom);**

- **подписването на ZSK и самото подписване на зоната, следва да се правят върху сигурна система, недостъпна отвън, а само резултата от подписването да се синхоронизира върху публично достъпните сървъри за имена;**

- **копия от KSK и ZSK двойките задължително трябва да се съхраняват на сигурно място, с цел предпазването им от изгубване.**

“Zone-walking” проблем и дискусията му:

- “zone-walking” проблем (?) в DNSSEC – на база NSEC записите може да се изтеглят всички ресурсни записи от дадена подписана зона;
- “zone-walking” проблем винаги е имало в DNS – напр. PTR съдържанието на in-addr.arpa зона може винаги да се изтегли пооктетно;
- BIND9 има механизми за разрешаване на безопасен зонален трансфер, така че да не се налага на заинтересованите да прибягват до “zone-walking” и да се предотврати DoS атака от множество паралелни трансфери;
- зоната на домейн не е хранилище на тайни, а масив с публична информация (!)
- предотвратяване на използването на NSEC – RFC4470 и “on-line signing”

Екстремни натоварвания при DNSSEC валидация:

- рекурсивните (кеширащите) сървъри за имена, извършващи DNSSEC валидация, следва да са с подходяща мощност и текущото им натоварване да бъде наблюдавано;
- огромният брой проверки на валидността на електронния подпис върху сървър с малка мощност, може да предизвика DDoS атака без умисъл;
- извършващите валидация кеширащи сървъри, подложени на голямо натоварване, трябва да използват многовъзлов режим на работа и да са разпределени в Мрежата чрез anycast.

Софийски Университет
"Св. Климент Охридски"

Колаборативни практики свързани с DNSSEC делегирания в БИОМ

Възможност за сътрудничество между СУ и БИОМ относно DNSSEC и практиките по използване и внедряване:

- **обмен на опит в използването на DNSSEC (уеб семинари);**
- **DNSSEC делегиране на acad.bg;**
- **DNSSEC базиран обмен на KSK публични ключове за участниците в БИОМ и създаване на йерархия;**
- **DNSSEC делегиране на in-addr.arpa домейни (LIR ACAD);**
- **DNSSEC базирани зони на DNSBL или други критични услуги свързани с DNS;**
- **рекурсивен/кеширащ сървър за имена с DNSSEC валидция за потребителите на БИОМ.**

? ВЪПРОСИ ?

⇦ МНЕНИЯ ⇨