DNSSEC для администратора домена

Сергей Мясоедов
NetArt Group

netart group

DNSSEC: зачем?

Главная задача – защита от атак

фальсификация данных DNS (атака Каминского)

Безопасность разрешения имён – в цепочке обеспечения безопасности
IP (secure routing) – DNSSEC – HTTPS

Дополнительные приятные функции (SSHFP) – в разработке

Почему именно так?

Единственная **надёжная** технология защиты

Криптоподсистема гибко настраивается и теоретически стойкая

Масштабирование оттестировано на DNS в рамках глобального Интернета

Внедрение DNSSEC

Каждая зона подписывается после изменения.

Используются два ключа (симметричная схема): KSK и ZSK

- ZSK – относительно часто изменяемый ключ
- KSK – редко изменяемый ключ, его изменение требует внесения изменений в родительскую зону (TLD)

У современных DNS-серверов никаких изменений в конфигурацию не вносится!

ПО DNS-сервера не нужно обновлять.

Трансформация зоны:

```
$ORIGIN net-art.cz.
$TTL 86400
@ IN SOA ns.net-art.cz. hm.net-art.cz. (2011053015 7200 1800 604800 86400)
 IN     NS      ns.net-art.cz.
 IN     NS      ns3.net-art.cz.
 IN     A       206.71.190.192
mail    IN      A       77.78.104.101
mail    IN      AAAA    2001:1528:137:2::2
```

```
$ORIGIN net-art.cz.
$TTL 86400
@ IN SOA ns.net-art.cz. hm.net-art.cz. (2011053015 7200 1800 604800 86400)

IN   RRSIG   SOA 5 2 86400 20111201200004 (20111101200004 19677 net-art.cz.
 DJO9r9XpDANWtkppBkpJGqeD/cRjAlzur9qO /mM4S7v6tf3uM/ae8zcYGZvxftkavxe+WUf3
 /tyY2097nrCTTetOCPAuZNpY7B4uChtXgCXY divr8uTQrpFM+FjjBhftZZzH5SLN5ieey/AX
 OtAQiMbiUxnnHmiazxDSnGHDTXI= )

IN     NS      ns.net-art.cz.
IN     NS      ns3.net-art.cz.

IN   RRSIG   NS 5 2 86400 20111201200004 (20111101200004 19677 net-art.cz.
 FfP45BiEB0zm0G/BxsZVLQs3pKKGvX4p/wyo tDx/TxecH4HA3PrZYbCsOkDIm1tNigEznsJx
 NxrW4yldi2Xkk2c1/4QDbkQzB/MSdqnc9qD+ de8B2pzJucDTRdMsv60sW+0BjsmzqOqoRdni
 G6L65DfEwGomBw3o6x0vf7oydZc= )
. . . .
```

Трансформация зоны:

```
> ls -l net-art.cz net-art.cz.signed
-rw-r--r--  1 root  wheel   1061 Nov  1 22:00 net-art.cz
-rw-r--r--  1 root  wheel  19986 Nov  1 22:00 net-art.cz.signed
```

Переподписание зоны

Поскольку ZSK – ключ короткого действия, нужно генерировать новый ключ до конца действия старого.

И уже с новым ZSK подписать зону и распространить её по NS, увеличив при этом serial.

Публикация DS

Хэш (дайджест) от неизменяемого KSK нужно поместить в родительскую зону:

```
net-art.cz.             IN DS 5536 5 1
7ED5A3CF770EF9276A65F1EFA686C79188EDAFE2

net-art.cz.             IN DS 5536 5 2
FD40614967D75F335895F23C6323B90F9559DBCC76E11435D27B8372 EDF84ED4
```

Теперь – чистая практика

Наборы утилит для работы с зонами:

- из дистрибутива BIND
- OpenDNSSEC
- DNSSEC-Tools.org

Подписание зоны:

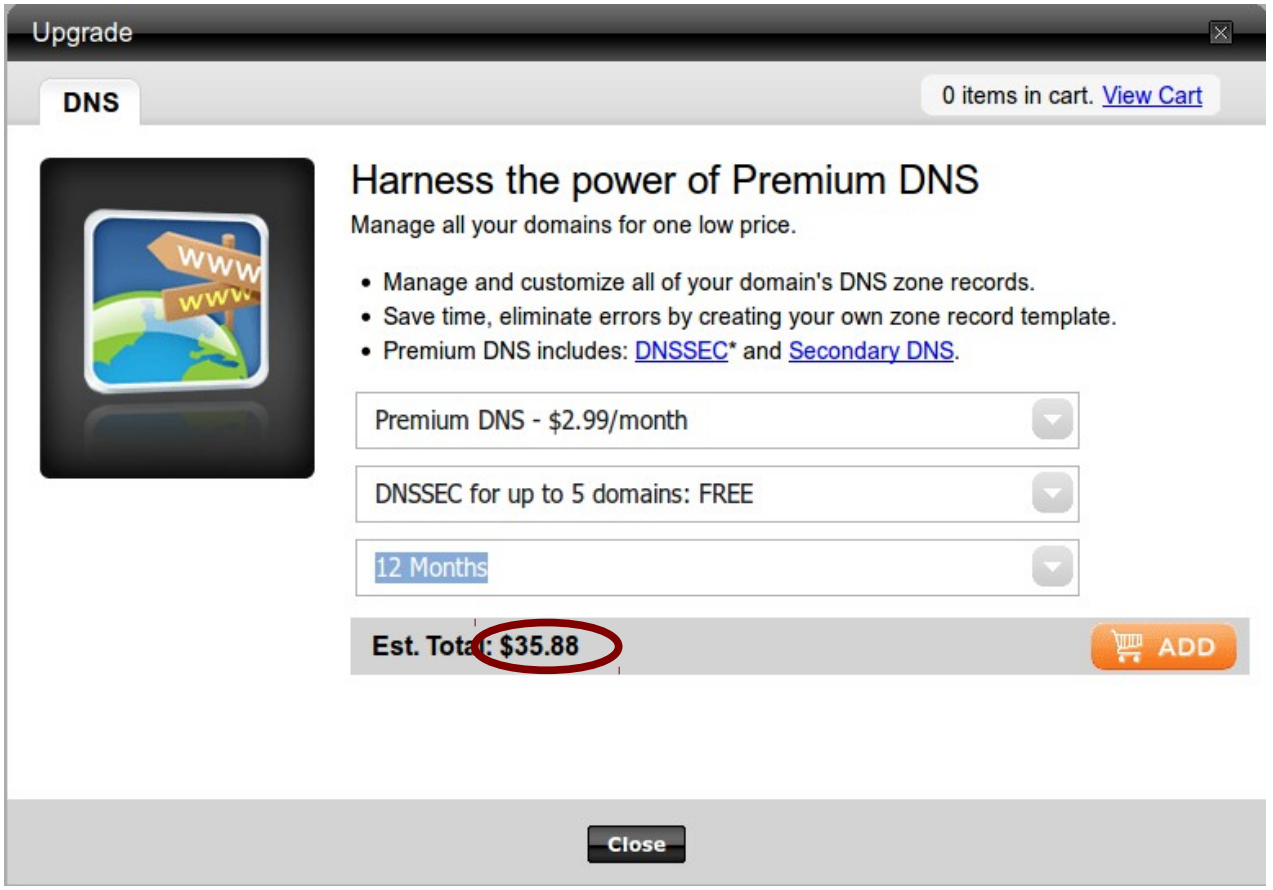
```
> zonesigner -genkeys net-art.cz
if zonesigner appears hung, strike keys until the program completes
(see the "Entropy" section in the man page for details)

Verifying the zone using the following algorithms: RSASHA1.
Zone signing complete:
Algorithm: RSASHA1: ZSKs: 2, KSKs: 1 active, 0 revoked, 0 stand-by

zone signed successfully

net-art.cz:
KSK (cur) 20032  -b 2048  11/01/11  (net-art.cz-signset-00003)
ZSK (cur) 52842  -b 1024  11/01/11  (net-art.cz-signset-00001)
ZSK (pub) 37221  -b 1024  11/01/11  (net-art.cz-signset-00002)


zone will expire in 30 days
DO NOT delete the keys until this time has passed.
>
```

Прикладной контроль DNSSEC

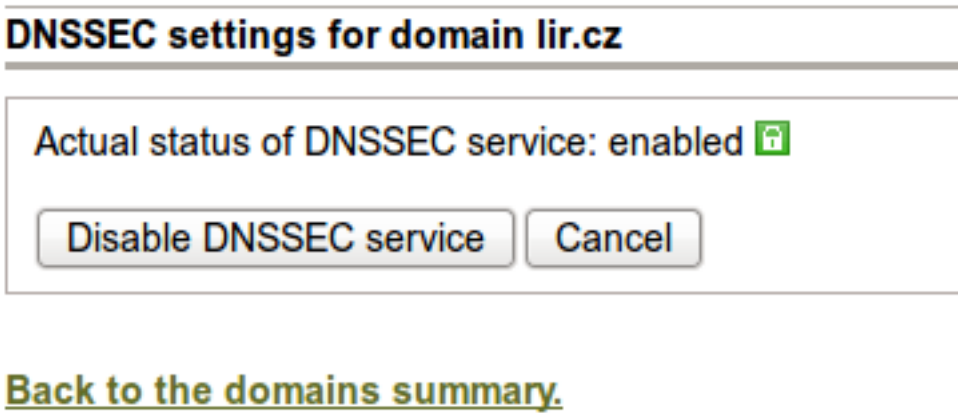
DNSSEC Validator
(www.dnssec-validator.cz)

Firefox plugin:

Admin's Option: Go Daddy



Admin's Option: Active24.cz



Admin's Option: RIPE NCC

```
> ripewhois -t domain | grep -v \%

domain:         [mandatory]  [single]     [primary/look-up key]
descr:          [mandatory]  [multiple]   [ ]
org:            [optional]   [multiple]   [inverse key]
admin-c:        [mandatory]  [multiple]   [inverse key]
tech-c:         [mandatory]  [multiple]   [inverse key]
zone-c:         [mandatory]  [multiple]   [inverse key]
nserver:        [optional]   [multiple]   [inverse key]
ds-rdata:       [optional]   [multiple]   [inverse key]
sub-dom:        [optional]   [multiple]   [inverse key]
dom-net:        [optional]   [multiple]   [ ]
remarks:        [optional]   [multiple]   [ ]
notify:         [optional]   [multiple]   [inverse key]
mnt-by:         [mandatory]  [multiple]   [inverse key]
mnt-lower:      [optional]   [multiple]   [inverse key]
refer:          [optional]   [single]     [ ]
changed:        [mandatory]  [multiple]   [ ]
source:         [mandatory]  [single]     [ ]
```

Admin's Option: выводы

Регистраторы:

- DNSSEC-хостинг как услуга
- полезная, но бесплатная опция для клиентов

Администраторы:

- самостоятельный хостинг зон
- DNSSEC-хостинг у своего регистратора
- услуги сторонних компаний

DS-записи в whois

```
> whois dnssec-with-gost.org | grep -A 10 Signed
DNSSEC:Signed
DS Created 1:17-Sep-2010 16:52:18 UTC
DS Maximum Signature Life 1:3456000 seconds
DS Key Tag 1:44448
Algorithm 1:12
Digest Type 1:1
Digest 1:63D18EB3CBEBB313C8F93D03EA3463F4B9A5A436
DS Created 2:17-Sep-2010 16:52:18 UTC
DS Maximum Signature Life 2:3456000 seconds
DS Key Tag 2:44448
Algorithm 2:12

> whois -h whois.ripe.net 248.130.188.in-addr.arpa | grep ds-rdata
ds-rdata:       15631 5 1 96E1418E6E72C26423C938AECECA318003C7AC44
ds-rdata:       15631 5 2 4ADECF3250C199886FCA4A5ED0E387A4E8B441CA
4B1644A1C5D1C7D7C81C8E93
```

CUI BONO?

Владельцы рисковой IT-инфраструктуры:

- Предприятия
- Платёжные системы
- Банки

Результат – спрос на DNSSEC-хостинг

Самостоятельный хостинг зон?

- Несложно настроить
- Не затратно
- Требует документирования
- Требует мониторинга

- Отказ может быть критичным

Регистраторы и TLD

- Работы *действительно* много
- Затратно, и расходы не окупятся в будущем
- Нужны технические писатели и переводчики
- Требует постоянного мониторинга
- Спрос пока мал

- Отказ может сломать ваш бизнес :-(

Регистраторы и TLD

На DNSSEC
~~много~~ денег не заработать.

Внедрять его – необходимо.

TLD: о чём думать на старте?

- Алгоритмы подписи
- NSEC/NSEC3
- Методы передачи DS в зону
- Методы проверок полученных DS
- Размеры зоны, её трансферы
- Частота подписи зоны
- Разделение расходов по внедрению

Вопросы?

kaa@net-art.cz