Упражнение: обновление ключа вручную

ЗАДАЧА

Мы собираемся обновить KSK для зоны, которую мы только что подписали.

НАПОМИНАНИЯ

- мы храним наши ключи в `/etc/namedb/keys/`
- там у нас сейчас хранится две (или более) пары ключей, одна пара для KSK и одна или более для ZSK.
Каждая пара представлена двумя файлами, один заканчивается на `".key"` (открытый ключ), и другой заканчивается на `".private"` (закрытый ключ)
- в корневой зоне есть набор записей DS, соответствующий нашему KSK

ОБНОВЛЕНИЕ KSK

Этот процесс довольно похож на обновление ZSK:

1. Перейдите в ключевой каталог:

```
$ cd /etc/namedb/keys/  
$ ls K*
```

2. Точно как в шаге 2 обновления ZSK, создайте новый KSK
Вам необходимо использовать параметр `"-f KSK"` для `dnssec-keygen`:

```
$ dnssec-keygen -f KSK -a RSASHA256 -b 2048 -n ZONE mytld
```

Вывод будет похож на:

```
Kmytld.+008+54511
```

3. Создайте набор записей DS для нового KSK.

```
$ cd /etc/namedb/keys/  
$ sudo dnssec-dsfromkey Kmytld.+008+54511.key > dsset-mytld-54511.
```

(здесь 54511 это идентификатор нового KSK, так что мы знаем, какой DS какому ключу соответствует).

На этой стадии мы можем решить, каким из двух методов производить обновление:

- Двойное подписывание

Мы добавляем новый KSK в набор записей DNSKEY, и мы подпишем ZSK, используя и текущий ("старый") KSK, и новый KSK. Через достаточный промежуток времени (время распространения, TTL, и т.д.) мы поменяем запись DS в родительской зоне на ту, которая содержит новый KSK. Валидаторы будут иметь оба KSK в кэше, и доверительная цепочка может быть проверена используя новый DS в родительской зоне.

- Предварительная публикация

Мы немедленно передаем DS для нового KSK в родительскую зону, и

публикуем ее вместе с существующим. Через достаточный промежуток времени, мы заменяем текущий ("старый") KSK на новый, и подписываем ZSK новым KSK. Валидаторы будут иметь оба DS в кэше, и доверительная цепочка может быть проверена.

Двойное подписывание используется чаще, потому что оно не требует чтобы родительская зона могла поддерживать несколько записей DS для каждой дочерней зоны. Дополнительно, несмотря на то, что это совершенно нормально, дополнительные DS с (пока) не опубликованными KSK в дочерней зоне могут привести к тому, что некоторые инструменты будут выдавать сообщения-предупреждения. Наконец, как указано в пункте 12 ниже, предварительная публикация требует два раза связываться с администратором родительской зоны (добавить новый DS, убрать старый DS), тогда как метод двойного подписывания требует связываться только один раз (замена одного DS на другой).

* Метод 1: Обновление KSK двойным подписыванием

4. Добавьте новый KSK в зону (отредактируйте файл):

Было:

```
$include "/etc/namedb/keys/Kmytld.+008+52159.key"; // KSK
```

Должно стать:

```
$include "/etc/namedb/keys/Kmytld.+008+52159.key"; // KSK старый  
$include "/etc/namedb/keys/Kmytld.+008+54511.key"; // KSK новый
```

Не забудьте также увеличить серийный номер.

5. Давайте подпишем зону старым и новым KSK (только ZSK будет подписан обоими KSK)

```
$ cd /etc/namedb/keys  
$ sudo dnssec-signzone -o mytld -k Kmytld.+008+oldksk -k Kmytld.+008+newksk  
../master/mytld Kmytld.+008+zsk  
  
$ sudo rndc reload mytld
```

6. Проверьте

```
$ dig @127.0.0.1 dnskey mytld +multi  
$ dig @127.0.0.1 dnskey mytld +dnssec +multi
```

7. Залогиньтесь в RZM и нажмите "Update". Вы заметите что RZM обнаружил ваш новый KSK. Проверьте что записи DS соответствуют содержимому файла dsset-mytd-newksk, который вы создали выше. Если все нормально, нажмите на "глаз" около SHA256, чтобы отметить его как действующий, потому пометьте старую запись DS для удаления. Нажмите "Update".

8. Проверьте с помощью dig - и до и после времени TTL (например, два раза по максимальному TTL зоны mytd и записи DS)

```
$ dig dnskey mytd +multi  
$ dig dnskey mytd +dnssec +multi
```

9. Уберите СТАРЫЙ KSK из файла зоны:

Было:

```
$include "/etc/namedb/keys/Kmytld.+008+52159.key"; // KSK старый
$include "/etc/namedb/keys/Kmytld.+008+54511.key"; // KSK новый
```

Должно стать:

```
$include "/etc/namedb/keys/Kmytld.+008+54511.key"; // KSK новый
```

Не забудьте также увеличить серийный номер.

10. Давайте подпишем зону только лишь новым KSK

```
$ cd /etc/namedb/keys
$ sudo dnssec-signzone -o mytld -k Kmytld.+008+newksk ./master/mytld Kmytld.
+008+zsk

$ sudo rndc reload mytld
```

11. Проверьте с помощью dig - и до и после времени TTL (например, два раза по максимальному TTL зоны mytld и записи DS)

```
$ dig dnskey mytld +multi
$ dig dnskey mytld +dnssec +multi
```

12. Обратите внимание на то, что двойное подписывание требует связываться с администратором родительской зоны только один раз, тогда как предварительная публикация требует двух сеансов.

* Метод 2: Обновление KSK предварительной публикацией

4. Закачайте набор записей DS для вашей зоны, либо используя web интерфейс, либо при помощи SCP, в зависимости от того, что сказал преподаватель.

Сообщите преподавателю, что вы закатали новый набор DS, и что вы хотите добавить его в корневую зону. Если вы использовали web интерфейс, это должно было произойти автоматически.

Если вы используете web интерфейс, залогиньтесь, как раньше.

В разделе "Edit Trust Anchor Details" введите метку ключа, дайджест, алгоритм, и типа дайджеста (из вывода на шаге 3 выше). Например,

```
mytld. IN DS 54511      8          2          983F33D43D1EBB069BF60...
          Метка Алгоритм Тип дайджеста Дайджест
                               RSASHA256
```

Уберите все пробелы из поля дайджеста и обратите внимание, что вам нужен только один "якорь доверия".

Нажмите "Update". Подождите минуту для распространения обновления.

5. Проверьте и перепроверьте, что новый DS опубликован в родительской (корневой) зоне вместе с существующим (вам придется подождать по крайней мере два раза по TTL прежде чем все кэши обновлены):

```
$ dig @10.20.0.230 DS mytld
```

```
...  
;; ANSWER SECTION:  
mytld 900 IN DS 52159 8 2 31F1...  
mytld 900 IN DS 54511 8 2 983F... // <-- новый KSK  
...
```

Поскольку оба DS теперь в кэше, мы можем обновить наш KSK.

Затем мы добавим новый KSK в файл зоны, и мы откомментируем (уберем) старый KSK:

Было:

```
$include "/etc/namedb/keys/Kmytld.+008+52159.key"; // KSK
```

Должно стать:

```
;$include "/etc/namedb/keys/Kmytld.+008+52159.key"; // KSK старый  
$include "/etc/namedb/keys/Kmytld.+008+54511.key"; // KSK новый
```

Не забудьте также увеличить серийный номер.

... обратите внимание, что мы просто убрали старый KSK - он нам более не нужен - обе записи DS есть в родительской зоне, так что нам достаточно иметь только один KSK, поскольку "на интернете" его DS уже известен.

6. Давайте подпишем зону новым KSK

```
$ cd /etc/namedb/keys  
$ sudo dnssec-signzone -o mytld -k Kmytld.+008+54511 ../master/mytld Kmytld.  
+008+45000
```

```
$ sudo rndc reload mytld
```

7. Проверьте с помощью dig - и до и после времени TTL (или сброса кэшей)

```
$ dig dnskey mytld +multi  
$ dig dnskey mytld +dnssec +multi
```

8. Дайте знать преподавателю, что вы хотите, чтобы старый DS был убран из корневой зоны (или уберите его сами с помощью web интерфейса)

9. Посидите и поразмышляйте о том, насколько этот процесс является сложным и раздражающим, и насколько лучше было бы если бы все обновления ключей делались автоматически.