

# Practical DNSSEC

ENOG 6 meeting

# Расписание

- Введение
- Принципы работы с ключами
- Практика: генерация ключей
- Практика: подписывание зоны
- Практика: публикация зоны
- Периодические задачи
- Другой софт
- Заключение

# DNSSEC

- Придуман инженерами для инженеров
- Единственная надёжная технология защиты DNS
- Неплохо масштабируется
- Поддерживается большими игроками
- Поддерживается основными DNS-серверами

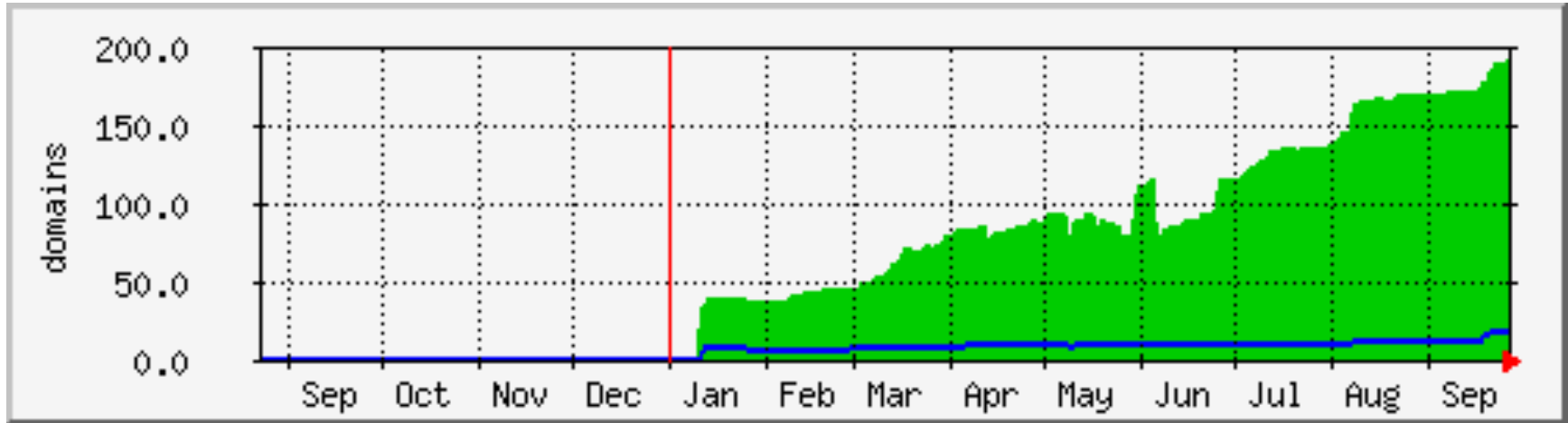
# Реализация в крупных TLD

Все крупные gTLD (.com, .net, .org etc) – поддерживают!

Многие крупные ccTLD (.de, .uk, .se, .ru) – поддерживают!

Регистраторы в .ru/.рф/.ua – увы ☹. Крайне мало. Возможно, я ошибаюсь?

# Статистика .ru / .рф



.ru – 192 домена

.рф – 17 доменов

# Статистика .ua

Всего 7 делегированных доменов с DS.

Динамику мы только начали отслеживать.

Динамика отсутствует.

Домены:

chernovtsy.ua, cv.ua, netassist.ua, nic.ua,  
rovno.ua, rv.ua, ua.ua

# Техника

- Документируем свои намерения, выбираем параметры криптографии и DNSSEC
- Генерируем ключи
- Помещаем ключи в свою зону
- Подписываем зону
- Публикуем DS через регистратора

# Ключи

- RFC 6781 рекомендует использовать два ключа: KSK и ZSK (sec. 3.1)
- Размер ключа в зависимости от криптоалгоритма – от 1 до 4096 бит
- Крайне рекомендуется содержать закрытые части ключей отдельно или даже в HSM. Но это затрудняет последующие манипуляции с ними.



# Поехали!

Bind 9.9 и тестовая зона enog.ru

Заходим по ssh/IPv4/IPv6:

```
username      enog
password      enog6
server        dns.enog.ru
```

.. и создаём свой рабочий каталог

```
mkdir mynickname; cd mynickname
```

.. копируем тестовую зону

```
cp /enog.ru .
```

# Процесс

- Только ключи, никаких сертификатов
- Bind 9.8/9.9 требует явного указания NSEC3 при генерации ключей
- Один ключ генерируем с параметром -f KSK
- Второй ключ – без этого параметра, и получится ZSK
- В итоге – 4 файла ключей, 2 из них готовы к включению в зону и уже имеют правильный origin

# На очереди – зона

- После запуска `dnssec-signzone` получим подписанную зону и файл с DS для публикации
- Если хотим NSEC3 – указываем `-3` и задаём SALT для хэш-функции
- На выходе имеем подписанную зону, которая как минимум в 4 раза больше неподписанной зоны с ключами, и в 25 раз больше оригинальной зоны.

# Сравним?

- Оригинальная зона
- Оригинальная зона с ключами
- Подписанная зона с NSEC
- Подписанная зона с NSEC3
- Наконец – DS-SET для передачи в родительскую зону

# Вариации

- Дополнительные флаги для Key Rollover:  
Revoked key
- NSEC3 не используется напрямую для криптографии DNSSEC – лишь для сокрытия указателя на следующую запись (Next SECure) для исключения перебора (walkthrough) зоны
- Для зон, похожих на нашу ENOG.RU, употребление NSEC3, пожалуй, избыточно

# Минималистский вариант

- Один ключ для подписи, KSK==ZSK
- Максимальный период валидности подписи – год, два, десять
- Одна DS-запись в TLD
- NSEC вместо NSEC3
- И ведь всё работает!
- Важно, чтобы хотя бы по одной цепочке DS-KSK-ZSK прошла успешная валидация, а сколько этих цепочек – не так уж и важно

# Оптимум?

- Настройки by default у bind (валидность подписей +30 дней с момента подписи)
- Другие разумные defaults у разных SW package
- Всё указанное хорошо работает у одного домена и неплохо масштабируется до десятков доменов
- Если нужно больше доменов – готового решения нет.
- Работа с зоной у ccTLD – вне нашего интереса.

# Немного в сторону

Chicken & egg problem:

- Валидация подписей основывается на моменте времени
- Может случиться, что после запуска системы время в CMOS не будет соответствовать реальности (например, 01:00 01 Jan 2010)
- Резолвинг даже NS, обслуживающих корневую зону, будет неуспешным
- До NTP-сервера таким образом достучаться не получится
- Выхода нет. Можно прописать IP-адрес NTP-сервера явным образом



# Публикация DS

Только два примера.

NIC.RU

GODADDY.COM

Буду рад показать и других регистраторов  
здесь.

# Автоматизация

- Переподписание зоны перед моментом инвалидирования RRSIG – критично и необходимо.
- Для хостеров – [пере] подписание большого количества зон одним KSK/ZSK.

# Хостерам

- Один KSK на много зон – удобно и эффективно
- Зоны придётся подписывать по одной сразу по окончании редактирования
- Все зоны придётся подписывать не позднее момента валидности RRSIG
- Придётся внедрять дополнительный мониторинг
- Не принесёт сразу никакого дохода
- Требуется наличие API у регистраторов для передачи DS в TLD
- Угрозы безопасности при использовании такой модели классические – компрометация ключа гораздо вероятнее успешной атаки на криптоалгоритмы

# Софт для автоматизации

- Я ещё не видел полноценных решений
- Моё решение не претендует на красоту, но работает
- В нём даже нет named-checkzone
- Один KSK и один ZSK для всех зон

<http://pastebin.com/KjBcvjiE>

# Валидация наших зон

Утилит довольно много, здесь только несколько производителей:

- NLnetLabs
- ISC
- CZ.NIC
- VERISIGN
- SurfNet

# Положение в .RU / .RF

Отчёт RU-CENTER (май 2013):

<http://stat.nic.ru/reports/whist-ru/dnssec.html>

Основной вывод – многие зоны (> 30%) не обслуживаются периодически.

Возможно, они были подписаны в качестве теста.

Вопросы?

Предложения?

Оценки?