Технический
Центр
Интернет

MSK IX

Опыт создания пилотной зоны DNSSec для RU

Ильин Александр
Начальник отдела сетевых технологий ТЦИ
kalend@tcinet.ru

RIPE regional meeting, 29.09.10-01.10.10

Технический Центр Интернет

MSK IX

Задачи пилотной зоны

- Разработка технического решения. Тестирование ПО разных поставщиков и их сравнительный анализ.
- Разработка требований к техническим ресурсам , требуемым для развертывания DNSSEC в штатном режиме
- Определение круга вопросов требующих разработки регулирующей документации
- Анализ готовности пользовательского ПО к использованию DNSSEC

Технический Центр Интернет

MSK IX

Тестовая зона DNSSec

Начало работы над проектом - конец 2009 года;

- Запуск лаборатории - февраль 2010;
- Сейчас завершена первая стадия проекта с 2 основными задачами:

1. Проверка готовности пользователей;
2. Сравнительный анализ продуктов, используемых в области DNSSec.

Технический Центр Интернет

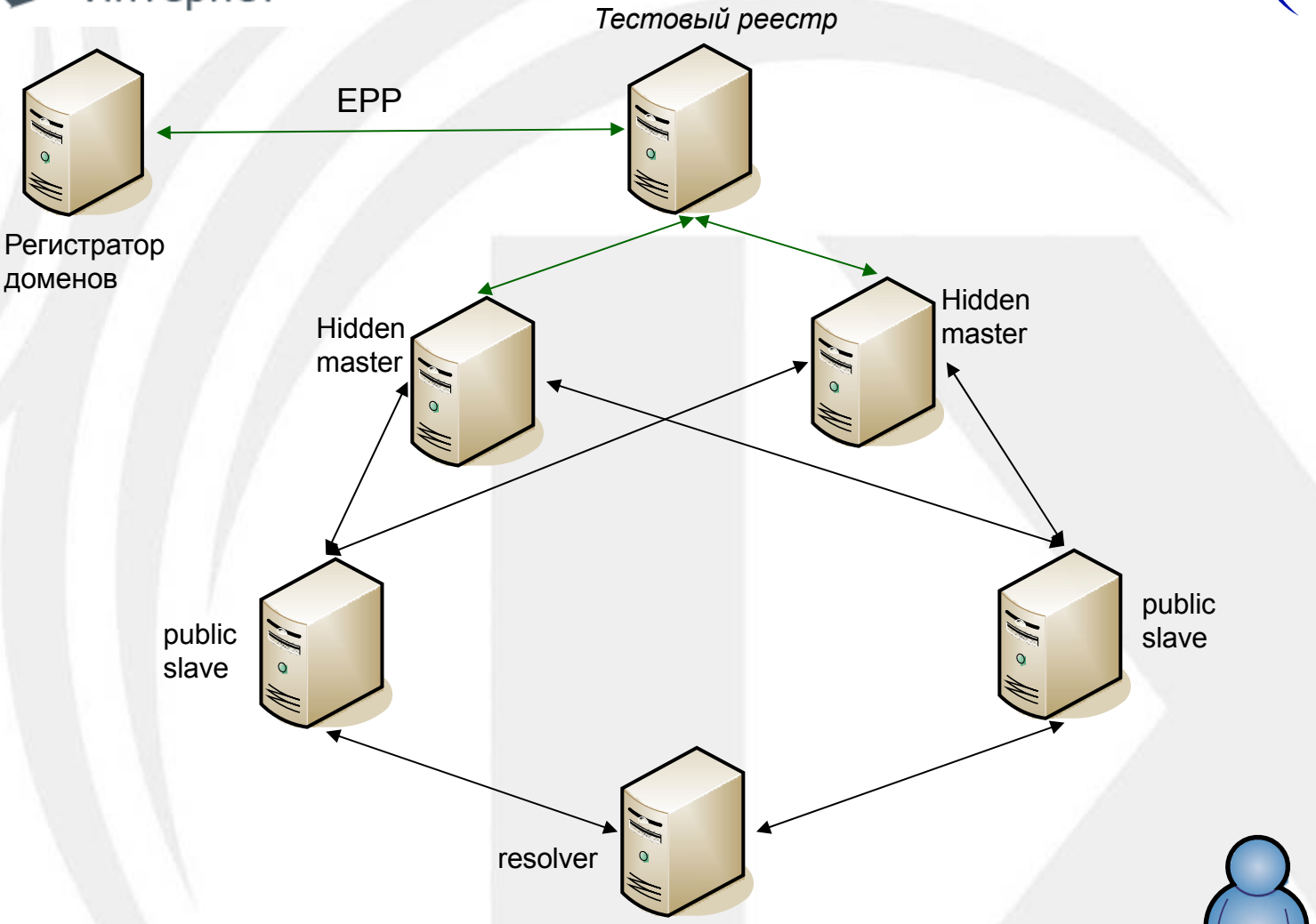
MSK IX

Этапы проекта

- Подготовительные работы (схема тестового стенда, методика тестирования, формат отчета, моделирование аварийных ситуаций, заказ оборудования, определение тестируемого ПО и т.д.)
- Построение опытной зоны
- Сравнительное тестирование ПО
- Определение алгоритма подписания зоны (система криптования)
- Определение методики ротации и публикации ключей
- Внесение в тестовый реестр TLD записи типа “DS” *(Delegation Signer)*, генерация тестовой зоны
- Комплексное тестирование с привлечением внешних пользователей
- Определение необходимых для штатной реализации технических параметров системы регистрации доменов (реестр, каналы и узлы сети DNS) .Разработка рекомендаций регистраторам по внесению DS-записей в реестр
- Составление отчета

Технический Центр Интернет

Схема тестового стенда



Технический Центр Интернет

MSK IX

ПО для тестов

1. *BIND* версия 9.7.1 (*ISC*) – широко распространенное ПО с открытым кодом;
2. *OpenDNSSEC* 1.1.0 (*OpenDNSSEC*) – используется многими европейских TLD (.DK, .FI, .NL, .SE, .UK);
3. *Ldns* 1.6.5 (*NLNet Labs*) – набор библиотек и утилит для работы с DNS;
4. *AlphaDNSSec* (*R-alpha*) – продукт отечественного разработчика, построенный на базе библиотеки ldns.

Технический Центр Интернет

Оборудование и Тестовая зона

MSK IX

Для тестов разного ПО выбрано однотипное оборудование:

CPU: Intel® Xeon® CPU L5520@2.27Ghz
Memory: 4Gb
HDD: 140Gb RAID1
OS: FreeBSD 8.0-RELEASE amd64

На момент тестирования RU содержала ~2600000, SU ~70000, РФ ~6000 доменов.

За основу была взята зона RU как наиболее интересная по размеру.

Технический Центр Интернет

Тестируемые критерии

MSK IX

- Наличие механизмов управления ключами;
- Поддержка алгоритмов: RSA (SHA-1, SHA-256, SHA-512), GOST R (34.10-2001, 34.11-94);
- Скорость подписывания зоны (RSA=1024bit, NSEC/NSEC3) с учетом роста;
- Скорость переподписывания зоны при росте количества записей на текущее среднесуточное значение и с учетом «всплесков».
- Удобство работы с продуктом (подписывание, переподписывание зоны, поддержка различных типов переподписывания).
- Возможность и необходимые условия для создания DLV (выделенной точки доверия)

Технический Центр Интернет

Исходные данные

MSK IX

- Выбор алгоритма (RSA поддерживается всеми серверами имен и резолверами, поддержка ГОСТа опциональна);
- Выбор длины ключей – компромисс между риском компрометации и производительностью. За основу взята рекомендуемая ANSI длина ZSK - 1024bit. Рекомендуемая длина KSK - 2048bit;
- Выбор типа последовательности (NSEC/NSEC3)

  NSEC – меньшее время подписи, поддерживается RSA и ГОСТ, скорость разрешения выше, существует возможность атаки zonewalk.

  NSEC3 – зашифрованный NSEC, не поддерживается ГОСТ, увеличенная нагрузка на авторитетные серверы и резолверы.

Технический Центр Интернет

Результаты

MSK IX

В лаборатории ПО BIND показало наилучшие результаты.

Отличительные особенности:

- Поддержка multithreading
- Поддержка динамических updates

Тестовое оборудование с RSA=1024bit и формирование NSEC3 с 10 итерациями: время подписи тестовой зоны ~36min. Увеличение памяти до 12Gb и удвоение количества ядер приводит к ускорению процесса до ~23min.

Несколько способов переподписывания у BIND:

1. «С нуля» - самый долгий, зона подписывается заново;
2. Добавление/удаление изменений в уже подписанный файл;
3. Динамические обновления: изменения «на лету» подписываются и синхронизируются с подписанной доменной зоной. Время переподписывания при добавлении 4000 и 25000 записей в зоне составило 9 секунд и 1 мин. 13 сек.

Технический Центр Интернет

Результаты

MSK IX

Обновление ключей:

Ключи ZSK/KSK должны обновляться, так как становятся уязвимыми со временем. Существуют плановые и чрезвычайные обновления.

Следует принять во внимание : чем меньше длина ключа, тем он уязвимее, большое кол-во данных в зоне упрощает процесс взлома ключа.

Исходя из этого (учитывая также опыт ANSI) – определяется частота обновления ZSK и KSK:

- ZSK, с помощью RSA длиной 1024bit = 3 месяца
- KSK, с помощью RSA длиной 2048bit = 1 год

Технический Центр Интернет

Требования к каналам связи

MSK IX

Были проведены тесты по распространение доменной зоны по вторичным серверам.

Получены следующие параметры:

- Тестовая зона (NSEC) 1.5Гб AXFR канал 50Mbit/sec – 4 мин
- Тестовая зона (NSEC3) 2.1Гб AXFR канал 50Mbit/sec – 5 мин 30 сек

Также было отмечено, что при подписи двумя ключами RSA и ГОСТ (NSEC) размер тестовой зоны составил ~4Гб

На основании этого даны рекомендации по каналам связи между master и slave серверами DNS.

Технический Центр Интернет

Взаимодействие с реестром

MSK IX

На основании опытной зоны согласованы и протестированы особенности работы с реестром:

- В экземпляре объекта домен могут находиться 1 или более DS-записей
- Сложность проверки реестром синтаксиса DS записей привела к обязательности указания DNSKEY.
- В структуре DS-записи все поля стандартные согласно RFC. Поле maxsiglife (максимальное время жизни подписи) является параметром реестра и его значение принято 605900.
- При переносе домена между регистраторами, входящие в него DS-записи не изменяются и переносятся вместе с доменом

Технический Центр Интернет

DLV

MSK IX

На этапе тестирования был также изучен механизм DLV:

- DLV можно использовать для тестирования DNSSec с привлечением внешних пользователей, не затрагивая реестр.
- Необходимые настройки выполняют только держатель DLV зоны; лицо, желающее использовать DLV для своей зоны; администратор резолвера, доверяющий DLV зоне и желающий использовать DNSSEC.
- Однако DLV не является заменой стандартной цепочки доверия, а скорее обеспечивает дополнительную возможность для валидации данных. Согласно RFC в первую очередь резолвер обязан использовать другие методы валидации.

Технический Центр Интернет

Итоги

MSK IX

1. Алгоритм — RSA.
2. Длина KSK — 2048 бит.
3. Время жизни KSK — 1 год;
4. Длина ZSK — 1024 бита.
5. Время жизни ZSK — 3 месяца;
6. Каналы между master и slave серверами не менее 50 мбит/сек;
7. В реестре должны быть реализованы возможности добавления DS записей, DNSKEY записей.
8. Нам необходима возможность добавления DNSKEY для TLDa.

Технический Центр Интернет

Внешнее тестирование

MSK IX

Составлена программа тестирования с привлечением внешних организаций:

- Исследование DLV
- С привлечением тестового реестра
- С использованием альтернативных тестовых серверов в качестве основных для валидации
- Исследование механизмов генерации и обновления ключей.
- Проверка функционирования DNSSec со стороны конечных пользователей.

Приглашаем желающих присоединиться к тестированию.

Технический Центр Интернет

Планы на будущее

MSK IX

1. Провести тестирование с внешними пользователями.
2. Организовать действующую тестовую зону DLV для сторонних пользователей.
3. Изучить возможность использования отечественных аппаратных ускорителей.
4. Определить порядок подписи зон и подготовиться к внедрению DNSSec.
5. Просветительская работа среди регистраторов, клиентов и т.д.

Технический
Центр
Интернет

MSK IX

Вопросы?