# Безопасность DNS

Филипп Кулин


Saint HighLoad++

# Откиньтесь на спинку кресла

- Эта презентация сделана с помощью LaTeX
- Я расскажу страшную сказку
- Я сделаю акцент на точку зрения роботов
- Несмотря на обыденность, тема DNS очень специфична
- Я рассмотрю какие-то инструменты

# DNS — всему голова

- Жизнь пользователей в сети
- Запросы к API, работа с CDN
- Облака, микросервисы, автообнаружение и конфигурация
- Невообразимое количество всего

# Тайная жизнь привычных программ

- SSHD определяет домен для подключившегося IP
  и этот факт является одним из источников седых волос у админов
- MySQL определяет домен для подключившегося IP
- Apache определяет домен для подключившегося IP
  даже если `HostnameLookups Off`, но есть `Require`
- Microsoft Windows постоянно шлет DNS Update в сеть
- Запустите tcpdump/WireShark

# DNS — это просто?

Три каверзных вопроса:

- Каков максимальный размер доменного имени?
- Точку на конце надо ставить?
- Что именно спрашивает ресолвер и что отвечают DNS-сервера при рекурсивном обходе?

# Как устроен DNS

здесь схемка

# Особенности классического DNS

- UDP транспорт. Нет соединения
- Нет идентификации серверов DNS
- Нет контроля данных
- Нет шифрования

# Угорозы в системе DNS

здесь схемка

# Заложенная в DNS безопасность

# Основные проблемы

- Подделка
  - Отравление
  - Взлом серверов и замена записей
  - Поддельные серверы, BGP-injection
- Прослушка
  - Шпионаж и промышленный шпионаж
    - … с использованием госрегулирования
  - Маркетинговые исследования
  - Система блокировок сайтов

# Защита от подделки

- Не «взлетевший» DNSCurve
- Расширение DNSSEC

# DNSCurve

Концепция

- Аутентификация авторитативного DNS-сервера
- Защита обмена между ресолвером и авторитативным сервером

Принцип действия

- Публичный ключ DNS-сервера с магическим префиксом "`uz5`" в NS-записи домена:

  **uz5**`qry75vfy162c239jgx7v2knkwb01g3d04qd4379s6mtcx2f0828.dnscurve.io`

- Защищенное соединение с DNS-сервером по специальному протоколу

# DNSCurve. Особенности

- Не меняет саму спецификацию DNS
- Основан на вере в целостность системы
- Зависит от источника ответа
- Внедрение отсутствует
- Представляет исключительно академический интерес
- **Это был экспериментальный стенд для ED25519**

# DNSSEC

- Концепция
  - Источник записи не важен. Используя доверенный корневой ключ возможно проверить любую подписанную запись
- Принцип действия
  - Записи зоны подписаны ключом зоны
  - Подтверждения подписи выстраиваются в цепочку доверия

# DNSSEC. Подпись зоны

картинка

# DNSSEC. Цепочка доверия

картинка

# DNSSEC. Особенности

- Требует аккуратности и непрерывного обслуживания даже в статическом состоянии
- Сложные реализации «отрицательного ответа»
- Большой размер ответа
- Крайне слабая глубина внедрения
- **Источник ответа не важен**

# DNSSEC. Использование

- Прозрачная проверка

  Потребитель получает фильтрованные ответы
- Явная проверка

  Потребитель явно указывает ресолверу, что хочет получить проверенный результат. Проверяет флаги ответа
- Усиленная проверка

  Потребитель проверяет подписи сам

# DNSSEC. Тренды

- Алгоритм ECDSA
  - скорость
  - небольшой размер ответов по сравнению с RSA
- Подпись «на лету»
  - использование «белой лжи»[1]
  - использование «чёрной лжи»[2]

# Вопросы

В любом случае пишите мне

schors@gmail.com

# Ссылки


[1] W. Mekking (NLnet Labs) R. Gieben (Google). *RFC 7129. Authenticated Denial of Existence in the DNS*. Определение белой лжи. Февр. 2014. https://datatracker.ietf.org/doc/html/rfc7129.

[2] Dani Grant (Cloudflare). *Economical With The Truth: Making DNSSEC Answers Cheap*. Определение черной лжи. 24 июня 2016. https://blog.cloudflare.com/black-lies/.

[3] *Beamer - Overleaf, Online LaTeX Editor*. https://www.overleaf.com/learn/latex/Beamer.

[4] Uri Nativ. *How to present code*. 2016. https://www.slideshare.net/LookAtMySlides/codeware.

[5] Филипп Кулин. *Пишем презентации в LaTeX*. 14 окт. 2019. https://habr.com/ru/post/471352/.