

# Безопасность DNS

Филипп Кулин



Saint  
**HighLoad++**



# Откиньтесь на спинку кресла

- Эта презентация сделана с помощью  $\text{\LaTeX}$
- Я расскажу страшную сказку
- Несмотря на обыденность, тема DNS очень специфична
- Я сделаю акцент на эксплуатацию сервисов

# 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

# 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

# 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`

# 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

# 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
- Docker, Kubernetes, etc



# 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
- Docker, Kubernetes, etc
- **Запустите tcpdump/WireShark**

# DNS — это просто?

Три каверзных вопроса:

- Каков максимальный размер доменного имени?

# DNS — это просто?

Три каверзных вопроса:

- Каков максимальный размер доменного имени?
- Точку на конце надо ставить?

# 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

# Угрозы в системе DNS

здесь схемка

# Заложенная в DNS безопасность



# Основные проблемы

- Подделка
  - Отравление
  - Взлом серверов и замена записей
  - Поддельные серверы, BGP-injection
  -

# 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
  -

# А так ли страшен чёрт?

# А так ли страшен чёрт?

- DNS-уязвимости не самоцель, часто нужны условия

# А так ли страшен чёрт?

- DNS-уязвимости не самоцель, часто нужны условия
- Однако DNS никогда не в одиночестве

# А так ли страшен чёрт?

- DNS-уязвимости не самоцель, часто нужны условия
- Однако DNS никогда не в одиночестве
- Ваш сетевой периметр защищен? Точно?

# А так ли страшен чёрт?

- DNS-уязвимости не самоцель, часто нужны условия
- Однако DNS никогда не в одиночестве
- Ваш сетевой периметр защищен? Точно?
- Ваша сеть получает подписанные маршруты?

# А так ли страшен чёрт?

- DNS-уязвимости не самоцель, часто нужны условия
- Однако DNS никогда не в одиночестве
- Ваш сетевой периметр защищен? Точно?
- Ваша сеть получает подписанные маршруты?
  - Вы ведете журнал странных анонсов?
- Ваши сервисы проверяют сертификат соединения?



# 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:  
`uz5qry75vfy162c239jgx7v2knkwb01g3d04qd4379s6mtcx2f0828.dnscurve.io`
- Обмен с DNS-сервером шифруется

# DNSCurve. Особенности

- Не меняет саму спецификацию DNS
- Основан на вере в целостность системы
- Зависит от источника ответа
- Внедрение практически отсутствует
- Шифрование на основе 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

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

# DNSSEC. Варианты использования

- 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»<sup>5</sup>
  - использование «чёрной лжи»<sup>6</sup>

# DNSSEC. Поддержка

- **Клиенты**

`dig, drill`

- **Ресолверы**

`systemd-resolved, dnsmask, unbound, KNOT Resolver, CoreDNS, PowerDNS recursor, BIND`

- **Авторитативные сервера DNS**

`KNOT, CoreDNS, PowerDNS, NSD, YADIFA, BIND`

- **Сервера DNS с подписью «на лету»**

`KNOT, CoreDNS, PowerDNS (частично)`

# Защита от прослушки DNS

Шифрование канала

# Защита от прослушки DNS

Шифрование канала

- DNSCrypt

# Защита от прослушки DNS

Шифрование канала

- DNSCrypt
- DNS-over-HTTPS Google API

# Защита от прослушки DNS

Шифрование канала

- DNSCrypt
- DNS-over-HTTPS Google API
- DNS-over-TLS
- DNS-over-HTTP/2
- DNS-over-QUIC

# Защита от прослушки DNS

Шифрование канала

- DNSCrypt
- DNS-over-HTTPS Google API
- DNS-over-TLS
- DNS-over-HTTP/2
- DNS-over-QUIC

Алгоритмы и фильтры

# Защита от прослушки DNS

## Шифрование канала

- DNSCrypt
- DNS-over-HTTPS Google API
- DNS-over-TLS
- DNS-over-HTTP/2
- DNS-over-QUIC

## Алгоритмы и фильтры

- Минимизация QNAME при запросах



# Защита от прослушки DNS

## Шифрование канала

- DNSCrypt
- DNS-over-HTTPS Google API
- DNS-over-TLS
- DNS-over-HTTP/2
- DNS-over-QUIC

## Алгоритмы и фильтры

- Минимизация QNAME при запросах
- EDNS0 Client subnets

# Шифрование канала

Защита канала сводится к двум задачам

- Аутентификация ресолвера
- Защита обмена между потребителем ресолвером

# DNSCrypt

- Настройка мастер-ключа и имени сервера
- Получение «короткого» ключа и сертификата
- Запросы к серверу, идентичные DNSCurve

# DNSCrypt. Особенности

- Не меняет спецификацию DNS
- Нет ни RFC, ни Draft. Только спецификация на сайте
- Имеет заметную программную поддержку
- Не предусмотрена замена мастер-ключа
- Не «взлетел»

# DNSCrypt. Поддержка

А надо?

# DNS-over-HTTPS (Google API)

Google предоставляет JSON-API к DNS

Страница с описанием:

<https://developers.google.com/speed/public-dns/docs/dns-over-https>

Массово используется для веб-приложений

# DNS-over-TLS (DoT)

# DNS-over-HTTPS (DoH)



# DNS-over-QUIC (DoQ)

# Реакционизм. Подделка

Картинка.

```
DDDDDDDDDDDDDDDDDDDDLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLL
HHHHHHHHHHHHHHHHHv GGGGGGGGGGGGGGGGGGGGGGGGGGGG
OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO
BNNNNNNNNNNNNNNN
```

# Реакционизм. Подделка

- Не позволяет подставлять «свой» ответ

# Реакционизм. Подделка

- Не позволяет подставлять «свой» ответ
  - Противоречит копоративным политикам

# Реакционизм. Подделка

- Не позволяет подставлять «свой» ответ
  - Противоречит копоративным политикам
  - Мешает спецслужбам проводить спецоперации

# Реакционизм. Подделка

- Не позволяет подставлять «свой» ответ
  - Противоречит корпоративным политикам
  - Мешает спецслужбам проводить спецоперации
- Переусложненное обслуживание приводит к ошибкам

# Реакционизм. Прослушка

Картинка Родина Слышит

# Реакционизм. Прослушка

- Не позволяет анализировать DNS-запросы



# Реакционизм. Прослушка

- Не позволяет анализировать DNS-запросы
  - Нарушает корпоративные стандарты безопасности

# Реакционизм. Прослушка

- Не позволяет анализировать DNS-запросы
  - Нарушает корпоративные стандарты безопасности
  - Мешает приложениям защиты отслеживать действия браузера

# Реакционизм. Прослушка

- Не позволяет анализировать DNS-запросы
  - Нарушает корпоративные стандарты безопасности
  - Мешает приложениям защиты отслеживать действия браузера
  - Создаёт видимость безопасности

# Реакционизм. Прослушка

- Не позволяет анализировать DNS-запросы
  - Нарушает корпоративные стандарты безопасности
  - Мешает приложениям защиты отслеживать действия браузера
  - Создаёт видимость безопасности
- Дополнительная нагрузка

# Реакционизм. Прослушка

- Не позволяет анализировать DNS-запросы
  - Нарушает корпоративные стандарты безопасности
  - Мешает приложениям защиты отслеживать действия браузера
  - Создаёт видимость безопасности
- Дополнительная нагрузка
- Цикл получения ответа неприемлемо долгий

# Реакционизм. Госрегулирование

Картинка с самураем и флажками/нашивками  
РКН/FCC/etc

# Реакционизм. Госрегулирование

- Большинство «госблокировок» в мире основано на DNS

# Реакционизм. Госрегулирование

- Большинство «госблокировок» в мире основано на DNS
- НСДИ РФ не совместима с DNSSEC



# Реакционизм. Госрегулирование

- Большинство «госблокировок» в мире основано на DNS
- НСДИ РФ не совместима с DNSSEC
- НСДИ РФ не поддерживает защиту

# Реакционизм. Госрегулирование

- Большинство «госблокировок» в мире основано на DNS
- НСДИ РФ не совместима с DNSSEC
- НСДИ РФ не поддерживает защиту
- Давление UK ISPA

# Многое осталось за кадром

- Обслуживание и эксплуатация DNSSEC, DoT/DoH
- Применение DNSSEC, SSHFP, DANE
- Обзор авторитативных серверов
- Обзор кэширующих серверов, включая `systemd.resolved`
- Инструменты
- `glibc` и `resolv.conf`
- ...

# Вопросы

Перед докладом я многое освежил в памяти, многое не вошло в доклад

В любом случае пишите мне

[schors@gmail.com](mailto:schors@gmail.com)

# Ссылки. DNSCurve

- [1] *DNSCurve.io - A Community for DNSCurve.* Основной сайт DNSCurve. <https://dnscurve.io/>.
- [2] *M. Dempsy. Link-Level Security for the Domain Name System.* 26 февр. 2010.  
<https://datatracker.ietf.org/doc/html/draft-dempsy-dnscurve-01>.
- [3] *Dq is a package with DNS/DNSCurve related software.* <https://mojzis.com/software/dq/>.
- [4] *World's fastest-to-synchronize Secondary DNS service.* Единственный известный DNS-сервис с поддержкой DNSCurve.  
<https://www.buddyns.com/>.

# Ссылки. DNSSEC

- [5] 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>.
- [6] Dani Grant (Cloudflare). *Economical With The Truth: Making DNSSEC Answers Cheap*. Определение черной лжи. 24 июня 2016. <https://blog.cloudflare.com/black-lies/>.
- [7] *Визуализация DNSSEC*. <http://dnsviz.net/>.
- [8] Филипп Кулин. *DNSSEC. Руководство регистратора доменов*. Дек. 2016. <https://www.slideshare.net/schors/dnssec-71055077>.
- [9] Филипп Кулин. *DNSSEC. Руководство оператора доменов*. Окт. 2017. <https://www.slideshare.net/schors/enog14-dnssec>.
- [10] *RFC 4033. Введение в DNSSEC*. Март 2005. <https://tools.ietf.org/html/rfc4033>.
- [11] *RFC 4034. Ресурсные записи для DNSSEC*. Март 2005. <https://tools.ietf.org/html/rfc4034>.
- [12] *RFC 4035. Модификации протокола DNS для DNSSEC*. Март 2005. <https://tools.ietf.org/html/rfc4035>.
- [13] *RFC 6781. Эксплуатация DNSSEC*. Дек. 2012. <https://tools.ietf.org/html/rfc6781>.
- [14] *RFC 7583. Соображения по ротации ключей DNSSEC*. Окт. 2015. <https://tools.ietf.org/html/rfc7583>.

# Ссылки. DNSCrypt

# Ссылки. DoH/DoT



# Ссылки. Разное

# Ссылки. L<sup>A</sup>T<sub>E</sub>X

- [15] *Beamer - Overleaf, Online LaTeX Editor.* <https://www.overleaf.com/learn/latex/Beamer>.
- [16] *Uri Nativ. How to present code.* 2016. <https://www.slideshare.net/LookAtMySlides/codeware>.
- [17] *Филипп Кулин. Пишем презентации в LaTeX.* 14 окт. 2019. <https://habr.com/ru/post/471352/>.