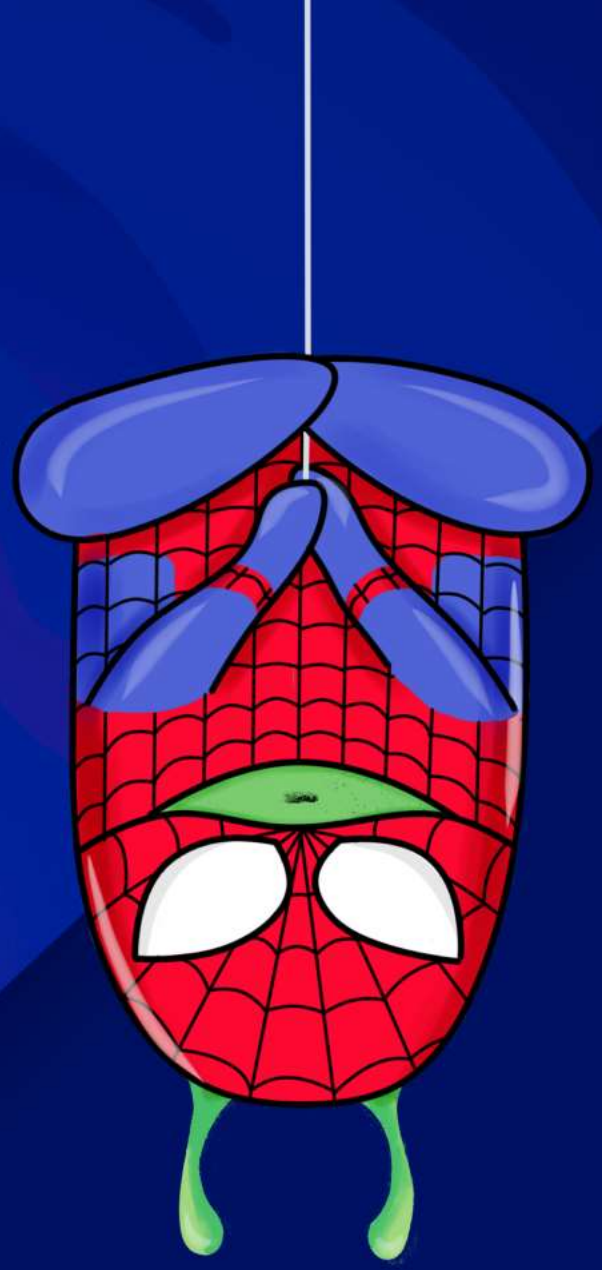
Безопасность DNS



Спикер:
Алексей Учакин

Два пути (не для видео)

- Безопасность сервера
- Безопасность клиента

БЕЗОПАСНОСТЬ DNS-СЕРВЕРА

rate-limits

доступ только к slave

поддержка tcp

ограничение видимости ответов

использовать провайдера DNS

БЕЗОПАСНОСТЬ DNS-КЛИЕНТА

- DoH / DoT / … - защита “последней мили”
- Используем защищённый транспорт: HTTPS, TLS, QUIC..
- Защищаемся от подмены DNS-ответов от сервера
- Полагаемся на то, что рекурсор нам отдаёт достоверные данные

БЕЗОПАСНОСТЬ DNS-КЛИЕНТА

DNSSec - проверка валидности ответа

Каждая запись и зона подписываются с помощью специальных ключей

Каждый ключ можно проверить с помощью вышестоящего сервера

Можно однозначно сказать, что ответ не был изменён “по дороге”

Нет гарантий от компрометации сервера

TL;DR

- **DNS** — «S» there is not for security
- Лучший способ **защитить DNS-сервер** — воспользоваться сервисом DNS-хостинга
- **DoT** и **DoH** — защищают трафик от клиента до рекурсивного сервера
- **DNSSec** — подтверждает подлинность записи, но имеет ограничения