Fake SNI indication: a way to cheat DPI

Dmitry Belyavskiy, Cryptocom.ru
IETF 104, Prague
March 26, 2019

DPI: how to deal with https?

Filter by IP — we can’t do anything with it

Filter by hostname in the certificate — impossible if TLS 1.3 in use

Encrypted SNI — may be suspicious itself

Whitelisting — very suspicious idea but still here

Fake SNI: why?

SNI indicates the host name, but it has not to be a true host name

Fake SNI: indication of the host name

Delivery: DNS

TLS (1.3) handshake looks normal

Reasonable fallback when ESNI is censored

Fake SNI vs aliases

Fake SNI goes for free

Relatively fast rotating — DNS record TTL

Easy to implement in code

Some future ideas

- Provide some rules of generating fake names
  (E.g. hash hmac_key_range tld)
- One-time Fake name
- Can we make something with delegated credentials?

Links

Draft: https://datatracker.ietf.org/doc/draft-belyavskiy-fakesni/

GitHub repo: https://github.com/beldmit/fakesni/

Questions?

beldmit@gmail.com