Measuring the Accessibility of Domain Name Encryption and its Impact on Internet Filtering

Nguyen Phong Hoang, Michalis Polychronakis, Phillipa Gill
Plaintext domains in network traffic

- **DNS query/response packets**
- **TLS handshake’s Client Hello**
- **Server Name Indication (SNI)**

- Security and privacy problems
- Susceptible to domain-based network filtering
Domain name encryption: DoT/DoH & ESNI

- **DoT**: DNS queries and responses are sent over a TLS tunnel using port 853 ([RFC7858](https://tools.ietf.org/html/rfc7858))

- **DoH**: DNS resolution is performed over HTTPS, inheriting all security benefits of the HTTPS protocol ([RFC8484](https://tools.ietf.org/html/rfc8484))

- **Encrypted SNI**: Starting from TLS1.3, the Server Name Indication extension in the Client Hello message during the TLS handshake can be *optionally* encrypted ([RFC8744](https://tools.ietf.org/html/rfc8744))

  → being reworked to Encrypted Client Hello ([Internet draft](https://tools.ietf.org/html/draft-kalb-tls13-encrypted-client-hello-a))
Domain encryption: DoT/DoH and ESNI

DoTH resolvers

HTTPS/TLS tunnel

blocked.domain?

(blocked.domain: 1.2.3.4)

TLS1.3 ClientHello

EncryptedSNI(blocked.domain)

HTTPS/TLS tunnel

ESNI-supported
blocked.domain

Domain encryption: DoT/DoH and ESNI
Motivation

Domain name encryption → better security and privacy

How about its impact on Internet filtering?

• Investigate whether domain name encryption technologies are being blocked by Internet filtering systems around the globe

• If not, can domain name encryption help with circumventing Internet censorship based on domain name information
DNEye

1) DNS Measurements
2) DoTH/ESNI Measurements

Raw Network Captures

20.7K VPN Gate vantage points

OONI  ICLab  Censored Planet

| Region     | Asia | Africa | America | Europe | Oceania |
|------------|------|--------|---------|--------|---------|
| Countries  | 32   | 4      | 15      | 32     | 2       |
| # of ASes  | 367  | 9      | 215     | 271    | 16      |
DNS-based Internet filtering is widespread

| Country       | Number of confirmed domains censored by DNS tampering |
|---------------|-------------------------------------------------------|
| China         | 300                                                   |
| Russia        | 205                                                   |
| Iran          | 147                                                   |
| Indonesia     | 134                                                   |
| India         | 98                                                    |

No major evidence of DNS-based filtering of DoTH at the AS level

- ordns.he.net blocked by China’s Great Firewall via DNS poisoning
- cloudflare-dns.com and mozilla.cloudflare.com in Thailand’s AS23969
China started blocking both DoT and DoH resolutions destined for popular DoTH resolvers from March 2021.
Blocking of DoT resolutions in China

- DNS over TLS is standardized in RFC7858 with 853 being used as the default port
- Port 853 is not used by other popular applications
  - Blocking the IP:853 pair is trivial and sufficient to hinder the use of DNS over TLS

| Time     | Source       | Destination    | Protocol | Info                                                                 |
|----------|--------------|----------------|----------|----------------------------------------------------------------------|
| 22:22:37... | 10.211.1.25  | 185.228.168.9  | TCP      | 36395 → 853 [SYN] Seq=1931890697 Win=64240 Len=0 MSS=1460            |
| 22:22:38... | 10.211.1.25  | 185.228.168.9  | TCP      | [TCP Retransmission] [TCP Port numbers reused] 36395 → 853           |
| 22:22:40... | 10.211.1.25  | 185.228.168.9  | TCP      | [TCP Retransmission] [TCP Port numbers reused] 36395 → 853           |
| 22:22:44... | 10.211.1.25  | 185.228.168.9  | TCP      | [TCP Retransmission] [TCP Port numbers reused] 36395 → 853           |
| 22:22:52... | 10.211.1.25  | 185.228.168.9  | TCP      | [TCP Retransmission] [TCP Port numbers reused] 36395 → 853           |
| 22:23:02... | 185.228.168.9 | 10.211.1.25   | TCP      | 853 → 36395 [RST, ACK] Seq=0 Ack=1931890698 Win=0 Len=0              |
Blocking of DoH resolutions in China

| No. | Source      | Destination | Protocol | Info                                                                 |
|-----|-------------|-------------|----------|----------------------------------------------------------------------|
| 1   | 10.211.1.25 | 8.8.8.8     | DNS      | Standard query 0x81d1 A dns.google OPT                              |
| 2   | 8.8.8.8     | 10.211.1.25 | DNS      | Standard query response 0x81d1 A dns.google A 8.8.8.8 A 8.8.4.4 OPT  |
| 3   | 10.211.1.25 | 8.8.8.8     | TCP      | 60915 → 443 [SYN] Seq=773598770 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=178 |
| 4   | 10.211.1.25 | 8.8.8.8     | TCP      | [TCP Retransmission] [TCP Port numbers reused] 60915 → 443 [SYN] Seq=773598770 |
| 5   | 10.211.1.25 | 8.8.8.8     | TCP      | [TCP Retransmission] [TCP Port numbers reused] 60915 → 443 [SYN] Seq=773598770 |
| 6   | 10.211.1.25 | 8.8.8.8     | TCP      | [TCP Retransmission] [TCP Port numbers reused] 60915 → 443 [SYN] Seq=773598770 |
| 7   | 10.211.1.25 | 8.8.8.8     | TCP      | [TCP Retransmission] [TCP Port numbers reused] 60915 → 443 [SYN] Seq=773598770 |
| 8   | 8.8.8.8     | 10.211.1.25 | TCP      | 443 → 60915 [RST, ACK] Seq=0 Ack=773598771 Win=0 Len=0               |

- DNS over HTTPS uses the popular 443 port
- IPs of popular DoH-supported DNS resolvers are widely known
  → Blocking the resolver_IP:443 pair is trivial and sufficient to hinder DNS over HTTPS services deployed by popular public resolvers
Centralized blocking of *.cloudflare-dns.com DoH resolvers in Saudi Arabia detected at different network locations
Decentralized blocking of ESNI Blocking in Russia

| No. | Time     | Source       | Destination  | Protocol | Info                                                      |
|-----|----------|--------------|--------------|----------|-----------------------------------------------------------|
| 288 | 18:40:2..| 172.17.0.2   | 104.21.86... | TCP      | 59808 → 443 [SYN] Seq=1116287061 Win=64240 Len=0 MSS=1460 SACK_PERM=1 |
| 293 | 18:40:2..| 104.21.86.223| 172.17.0.2   | TCP      | 443 → 59808 [SYN, ACK] Seq=2706902954 Ack=1116287062 Win=65535 Len=0 |
| 294 | 18:40:2..| 172.17.0.2   | 104.21.86... | TCP      | 59808 → 443 [ACK] Seq=1116287062 Ack=2706902955 Win=64256 Len=0 |
| 295 | 18:40:2..| 172.17.0.2   | 104.21.86... | TLSv1    | Client Hello                                             |
| 296 | 18:40:2..| 104.21.86.223| 172.17.0.2   | TCP      | 443 → 59808 [RST, ACK] Seq=2706902955 Ack=1116287755 Win=67584 Len=0 |
| 297 | 18:40:2..| 104.21.86.223| 172.17.0.2   | TCP      | 443 → 59808 [RST, ACK] Seq=2706902955 Ack=1116287755 Win=67584 Len=0 |
| 298 | 18:40:2..| 104.21.86.223| 172.17.0.2   | TCP      | 443 → 59808 [RST, ACK] Seq=2706902428 Ack=1116287755 Win=67584 Len=0 |
| 306 | 18:40:2..| 104.21.86.223| 172.17.0.2   | TCP      | 443 → 59808 [RST, ACK] Seq=2706902428 Ack=1116287755 Win=67584 Len=0 |
| 330 | 18:40:2..| 104.21.86.223| 172.17.0.2   | TCP      | 443 → 59808 [RST, ACK] Seq=2706902955 Ack=1116287755 Win=67584 Len=0 |

**Extension:** encrypted_server_name (len=366)

- **Type:** encrypted_server_name (65486)
- **Length:** 366
- **Cipher Suite:** TLS_AES_128_GCM_SHA256 (0x1301)
- **Key Share Entry:** Group: x25519, Key Exchange length: 32
- **Record Digest Length:** 32
- **Record Digest:** 6f8b000d384ae806bfccac2eb71a336e0629802999bf85c6b84c83d9ed0d548
- **Encrypted SNI Length:** 292
- **Encrypted SNI:** a3e11c7d9deefed9734ec58aabbff904031478a1bf6b4bc1f178c75c238bd672763378326...

**Extension:** record_size_limit (len=2)

0170 00 01 02 03 02 04 ff ce 01 6e 00 00 00 01 0d 0d 00 81
0180 00 04 03 06 03 07 05 0b 0c 0e 0f 01 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e 0f 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50 51 52 53 54 55 56 57 58 59 60 61 62 63 64 65 66 67 68 69 70 71 72 73 74 75 76 77 78 79 80 81 82 83 84 85 86 87 88 89 90 91 92 93 94 95 96 97 98 99 0a 0b 0c 0d 0e 0f 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50 51 52 53 54 55 56 57 58 59 60 61 62 63 64 65 66 67 68 69 70 71 72 73 74 75 76 77 78 79 80 81 82 83 84 85 86 87 88 89 90 91 92 93 94 95 96 97 98 99 

Decentralized blocking of ESNI connections in Russia based on the 2-byte signature ff ce of Encrypted SNI protocol
Filtering circumvention with domain name encryption

| Country | Circumvented/Total crawled | Other filtering techniques |
|---------|---------------------------|---------------------------|
|         | TCP | HTTP | TLS | SS |
| China   | 130/230 | 11   | 2   | 84 | 3 |
| Russia  | 53/56 | 1    | 1   | 1  | 0 |
| Iran    | 0/49 | 1    | 1   | 47 | 0 |
| Indonesia | 93/98 | 2    | 2   | 0  | 1 |
| India   | 20/20 | 0    | 0   | 0  | 0 |

- Encrypting DNS can help bypassing DNS-based censorship
- Not all domains support encrypted SNI
  → still susceptible to SNI-based blocking
Key takeaway

• Domain name encryption can help to partially circumvent Internet censorship based on DNS

• Notorious censors have already taken a step ahead to hinder the deployment of domain name encryption by
  ✓ blocking DoTH servers
  ✓ blocking ESNI connections

  => Domain name encryption protocols should be designed and deployed in a way such that blocking their traffic is not an option without causing large collateral damage

• SNI-based blocking is still possible as encrypted SNI has not been widely adopted
  => Encrypted Client Hello should be adopted universally