Network Working Group
Internet-Draft
Intended status: Experimental
Expires: August 24, 2019

TCI

February 20, 2019

# Fake Server Name Indication
# draft-belyavskiy-fakesni-01

Abstract

The document provides a specification of the Fake Server Name Indication. Being implemented, the Fake SNI specification provides a way to work around the monitoring solutions without providing any additional information to external observers.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on August 24, 2019.

## 1. Introduction

Many DPI solutions use SNI information as a criterion to filter connection to various sites. Though Encrypted SNI makes impossible to read the SNI value, there is information [1] that absence of SNI looks suspicious itself and all communications are blocked.

This specification introduces a way to provide a value of SNI treated by TLS server as an alias to one of the names known by server but not matching the possibly suspicious hostname.

This specification does not save from DPI solutions but it provides one more loophole to cheat them.

## 2. Fake SNI design goals

The solution specified in this document is inspired by the design of Encrypted SNI.

The provider publishes a name matching the target name to be provided in the clear text. This document defines a publication mechanism using DNS, but other mechanisms are also possible.

When a client wants to establish a TLS connection to a domain served by a Fake SNI-supporting provider, it replaces the value in "server_name" extension in the ClientHello with the value obtained by transport. The provider can then find out the desired name from its configuration and either establish the connection with the desired host or reject it.

## 3. Definitions

Original name - the hostname of service that is subject to hide.

Fake name - the hostname specified by server and sent by client to indicate intention to connect to host with original name.

## 4. Fake SNI indication

Fake SNI information is published in DNS via TXT RR. For example, the Fake SNI record for domain example.com may look like

_fakesni.example.com. 60S IN TXT "myfakerecord.com IP"

where IP address may be omitted. If present, it MUST match an IP address specified in A/AAAA record for the domain.

Value specified in the Fake SNI RR MUST NOT match any hostname available for the IP address it is valid for. Fake names for different hosts MUST be different.

## 5. Server behaviour

On receiveing the value of known Fake SNI in the TLS ClientHello server MUST return the certificate matching the original hostname. Otherwise server SHOULD abort the connection.

## 6. Client behaviour

Client MAY use the Fake SNI record as fallback if connecting using ESNI is blocked. In this case client initiates normal TLS connection specifying the value from Fake SNI record in the server_name extension. If the certificate received from server does not match the original hostname, the client MUST abort the connection. Otherwise the client MUST follow the normal process of TLS handshake.

## 7. Security considerations

As Fake SNI can be used in TLS 1.2, it does not provide any problems to DPI because in this case the original hostname is available in clear text in server certificate. TLS 1.3 encrypts the Certificate message, so it is RECOMMENDED to use Fake SNI together with TLS 1.3. To strengthen the protection, it's recommended to obtain _fakesni RR via DoT or DoH.

As DPI solutions are able to obtain the DNS _fakesni records as legitimate clients do, it is RECOMMENDED to set reasonable TTL values for the _fakesni records. Also it is RECOMMENDED to use such values of fake names that are syntactically correct domain names. Otherwise DPI can recognise the fake names as fake ones.

## 8. References

### 8.1. URIs

[1] https://mailarchive.ietf.org/arch/msg/tls/WiT3oEh6PO96mm0z28BNMp0YgGs

Author's Address

Dmitry Belyavskiy
Cryptocom LTD
Kedrova st, 14/2
Moscow 127083
RU

Email: beldmit@gmail.com