On the Importance of Encrypted-SNI (ESNI) to Censorship Circumvention

Zimo Chai, Amirhossein Ghafari, Amir Houmansadr

University of Massachusetts Amherst
What is SNI?
Server Name Indication (SNI) allows web-hosts to render the correct certificate
Server Name Indication (SNI) allows web-hosts to render the correct certificate.
Server Name Indication (SNI) allows web-hosts to render the correct certificate

Website A's Digital Certificate

ClientHello, SNI="a.com"

a.com
b.com
Server Name Indication (SNI) allows web-hosts to render the correct certificate.
Server Name Indication (SNI) allows web-hosts to render the correct certificate

- ClientHello, SNI="a.com"
- ClientHello, SNI="b.com"
TLS 1.2: SNI and CA are NOT encrypted...

ClientHello, SNI="a.com"

ClientHello, SNI="b.com"

Website A's Digital Certificate

Website B's Digital Certificate
TLS 1.2: SNI and CA are NOT encrypted...

ClientHello, SNI="a.com"

SNI=a.com
CA=a.com

Website A's
Digital
Certificate

a.com
b.com

unencrypted
encrypted
TLS 1.2: SNI and CA are NOT encrypted...

SNI=a.com
CA=a.com

Website A's Digital Certificate

ClientHello, SNI="a.com"

RST

a.com
b.com
Timeline: TLS 1.3 is finalized

TLS 1.3 finalized

3/21/2018
TLS 1.3: SNI is still NOT encrypted...

Website A's Digital Certificate

ClientHello, SNI="a.com"

Website B's Digital Certificate

ClientHello, SNI="b.com"

unencrypted

certified
Censors exploit SNI for censorship

South Korea is Censoring the Internet by Snooping on SNI Traffic

By Sergiu Gatlan
Circumvention: Domain Fronting

Server

Client

server_name: unblocked.com
certificate: unblocked.com

Censor

TLS 1.2

Encrypted

Unencrypted

TLS ClientHello with SNI

TLS ServerHello with Certificate

Client

Server

14
Circumvention: Domain Fronting

Server

Client

TLS 1.2

TLS ClientHello with SNI

TLS ServerHello with Certificate

GET / HTTP/1.1
Host: blocked.com

HTTP Response

server_name: unblocked.com
certificate: unblocked.com

Encrypted

Unencrypted
Timeline: CDNs Cease Domain Fronting

- TLS 1.3 finalized
- Amazon announced an end to Domain Fronting
- DNS-over-HTTPS added to Firefox 60.0
- 3/21/2018
- 4/2/2018
- 4/13/2018
Timeline: CDNs cease domain fronting

- TLS 1.3 finalized
- Amazon announced an end to Domain Fronting
- DNS-over-HTTPS added to Firefox 60.0
- Google announced an end to Domain Fronting
Timeline: ESNI is proposed for TLS 1.3

- TLS 1.3 finalized
- Amazon announced an end to Domain Fronting
- First ESNI Internet Draft
- DNS-over-HTTPS added to Firefox 60.0
- Google announced an end to Domain Fronting
Timeline: Cloudflare supports ESNI

- DNS-over-HTTPS added to Firefox 60.0
  - 3/21/2018

- Amazon announced an end to Domain Fronting
  - 4/2/2018

- Google announced an end to Domain Fronting
  - 4/13/2018

- First ESNI Internet Draft
  - 4/30/2018

- TLS 1.3 finalized
  - 7/2/2018

- Cloudflare started supporting ESNI
  - 9/24/2018
Timeline: Firefox supports ESNI

- TLS 1.3 finalized
- DNS-over-HTTPS added to Firefox 60.0
- Amazon announced an end to Domain Fronting
- Google announced an end to Domain Fronting
- First ESNI Internet Draft
- Cloudflare started supporting ESNI
- ESNI added to Firefox Nightly
How ESNI works?
How ESNI works?

- DNS over HTTPS/TLS
- Encrypted
- CDN Edge Server
- Censor
- Client
- TLS 1.3
How ESNI works?

DNS over HTTPS/TLS

Encrypted

DNS Server

DNS TXT Query

DNS TXT Result

Client

TLS 1.3

CDN Edge Server

DNS query: saf3241@vasdf3213ff....
How ESNI works?

1. **DNS over HTTPS/TLS**
2. **DNS TXT Query**
3. **DNS TXT Result**
4. **CDN Edge Server**
5. **TLS 1.3**
6. **Censor**
7. **Client**

**DNS query:** saf3241@vasdf3213ff....

Encrypted
How ESNI works?

1. **DNS over HTTPS/TLS**: Client performs a DNS query to a DNS server.
   - **DNS query**: saf3241@vasdf3213ff....
   - **encrypted_server_name**: f9jkl3zq....
   - **Encrypted DNS TXT Query**: DNS TXT result is sent to the client.

2. **TLS ClientHello with ESNI**: Client sends a TLS ClientHello message, including the ESNI extension.
   - **TLS 1.3**: Client and CDN Edge Server establish a TLS connection.

3. **TLS ServerHello**: CDN Edge Server sends a TLS ServerHello message.
   - **CDN Edge Server**}

The diagram illustrates the process of how ESNI (Encrypted Site Name Indication) works, demonstrating the flow from DNS to TLS connection establishment with the inclusion of ESNI to protect the server name.
Research Questions
Research Questions

● How many websites are supporting ESNI?

● How many currently censored websites in China can be unblocked with the help of ESNI?

● Is there any censor already censoring ESNI traffic?
How many websites are supporting ESNI?
How many sites are supporting ESNI?

As of August 2019, Cloudflare is the only CDN provider supporting ESNI.

Cloudflare provides an informative debugging page for every site using its CDN service.
How to know if a site supports ESNI?
Cloudflare debugging page

```
fl=102f16
h=chinadigitaltimes.net
ip=........................................
ts=1566939154.141
visit_scheme=https
uag=Mozilla/5.0 (X11; Fedora; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
colo=PHL
http=http/2
loc=US
tls=TLSv1.3
sni=encrypted
warp=off
```
Cloudflare debugging page

```
fl=102f16
h=chinadigitaltimes.net
ip=
ls=1566939154.141
visit_scheme=https
uag=Mozilla/5.0 (X11; Fedora; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
colo=PHL
http=http/2
loc=US
tls=TLSv1.3
sni=encrypted
warp=off
```
How many sites are supporting ESNI?

Location: On a VPS located in US

ESNI Enabled
How many sites are supporting ESNI?

Location: On a VPS located in US

ESNI Enabled

Alexa Top 1 Million Sites
Websites Supporting ESNI

More than 10% of Alexa Top 1 Million sites are supporting ESNI!
### Result: SNI Status and TLS Version

<table>
<thead>
<tr>
<th>SNI Status</th>
<th>TLS Version</th>
<th>Number</th>
<th>Portion</th>
</tr>
</thead>
<tbody>
<tr>
<td>encrypted</td>
<td>TLS1.3</td>
<td>101,190</td>
<td>92.56%</td>
</tr>
<tr>
<td>plaintext</td>
<td>TLS1.3</td>
<td>1,288</td>
<td>1.17%</td>
</tr>
<tr>
<td></td>
<td>TLS1.2</td>
<td>6,825</td>
<td>6.24%</td>
</tr>
<tr>
<td>off</td>
<td>TLS1.2</td>
<td>5</td>
<td>0.005%</td>
</tr>
<tr>
<td></td>
<td>-</td>
<td>14</td>
<td>0.012%</td>
</tr>
<tr>
<td>Total</td>
<td></td>
<td>109,322</td>
<td>100%</td>
</tr>
</tbody>
</table>
ESNI adoption with Sites Popularity

% Websites Supporting ESNI

Websites Grouped by Rank

Ranking (Millions)
Research Questions

● How many websites are supporting ESNI?

● How many currently censored websites in China can be unblocked with the help of ESNI?
How websites are censored in China?
Major Censorship techniques in China

- DNS Hijacking
- IP Blocking
- SNI Filtering
Detect DNS Hijacking - Result

Host without DNS resolving functionality located in China

GFW DPI

Probing Machine located in US

Alexa Top 1 Million Sites

unblocked.com?

blocked.com?

Forged Reply

Mark blocked.com as under DNS-Hijacking
Detect DNS Hijacking - Result

24,128 domains under DNS-Hijacking

Host without DNS resolving functionality located in China

GFW DPI

Probing Machine located in US

unblocked.com?

blocked.com?

Forged Reply

Mark blocked.com as under DNS-Hijacking
Detect SNI Filtering - Setup

Host with open ports located in China

GFW DPI

dport=3001
SNI='unblocked.com'

dport=3002
SNI='blocked.com'

Forged RST

Probing Machine located in US

Alexa Top 1 Million Sites

Mark blocked.com as under SNI-Filtering
Detect SNI Filtering - Result

- 21,446 domains under SNI-Filtering

Diagram:
- Host with open ports located in China
- GFW DPI
- Probing Machine located in US
- dport=3001, SNI='unblocked.com'
- dport=3002, SNI='blocked.com'
- Forged RST
- Mark blocked.com as under SNI-Filtering
Detect IP Blocking - IP List

Alexa Top 1 Million Sites

Resolve from Hong Kong

DNS

Select the first IP in an answer
Detect IP Blocking - IP List

Alexa Top 1 Million Sites

Resolve from Hong Kong

DNS

Select the first IP in an answer

539,456 unique IPs
Detect IP Blocking - Setup

Probing Machine located in China

Censor Router

IP=172.217.11.46

Probing Machine located in US

SYN
dport = 80,443

SYN/ACK

dport = 80,443

? + ✅ = ⏰
Detect IP Blocking - Result

39,787 domains under IP-Blocking
47,069 sites censored among Alexa Top 1M

- **24,128** domains under DNS-Hijacking (51.2%)
- **21,446** domains under SNI-Filtering (45.6%)
- **39,787** domains under IP-Blocking (84.5%)
Domains under different censorship

- Blocked by DNS Hijacking: 2514, 4698, 22,859
- Filtered by SNI: 250, 16,666
- Blocked by IP: 70, 12
Domains under different censorship

70 sites are exclusively under SNI - Filtering

- Blocked by DNS Hijacking: 2514
- Filtered by SNI: 4698
- Blocked by IP: 22,859
- Filtered by SNI - Blocked by IP: 16,666
- DNS Hijacking - Filtered by SNI - Blocked by IP: 250
- DNS Hijacking - Blocked by IP: 12
- Filtered by SNI - Blocked by IP: 70
Domains under different censorship

84.5% censored websites remain blocked in China
Effectiveness of ESNI
Effectiveness of ESNI

- 101,200 domains supporting ESNI
- 21,446 domains under SNI-Filtering
- 24,128 domains under DNS-Hijacking
- 39,787 domains under IP-Blocking

Legend:
- ESNI Supported
- DNS Hijacking
- SNI Filtering
- IP Blocking
Assume DNS-based censorship evaded

- 101,200 domains supporting ESNI
- 21,446 domains under SNI-Filtering
- 39,787 domains under IP-Blocking
- 0 domains under DNS-Hijacking
Current Effectiveness of ESNI

66 sites can be unblocked by ESNI

Censored websites VS. ESNI supporting websites
Current Effectiveness of ESNI

66 sites can be unblocked by ESNI

Censored websites VS. ESNI supporting websites

Support ESNI
Filtered by SNI
Blocked by IP

medium.com
boxun.com
chinnadigitaltimes.net
bannedbook.org
rsf.org
amnesty.org.au
....
ESNI increases the cost of blocking 101k sites

Censored websites VS. ESNI supporting websites
IPs belong to CDN edge server are blocked

Censored websites VS. ESNI supporting websites
Monitoring ESNI-based Censorship
Any area already censoring ESNI traffic?

Nick Sullivan @grittygrease

And it looks like they're blocking encrypted SNI outright (according to accounts on the ground). In some ways, this is our fault for not agreeing on a final spec and pushing it out to more clients faster. The politics around network privacy engineering are tricky. Cliffs abound.

Joseph Lorenzo Hall, PhD @JoeBeOne

Looks like South Korea has started filtering the internet across all ISPs using SNI (one thing we can't yet encrypt under TLS 1.3). Fuuuuuuck bugzil.la/1494901#c3 #censorship

7:48 PM - 12 Feb 2019
Monitoring ESNI-based Censorship from 14 Different Areas
Monitoring ESNI-based Censorship - Setup

ESNI Enabled

Sites supporting ESNI
Monitoring from 14 Different Areas

No ESNI-based Censorship Detected!
Conclusions
Conclusions

- 10% websites among Alexa Top 1M are supporting ESNI.
Conclusions

- **10%** websites among Alexa Top 1M are **supporting ESNI**.
- **84.5%** currently censored websites will **remain blocked** in China even if DNS- and SNI-based censorship are evaded.
Conclusions

● 10% websites among Alexa Top 1M are supporting ESNI.

● 84.5% currently censored websites will remain blocked in China even if DNS- and SNI-based censorship are evaded.

● Only 66 websites currently censored in China can be unblocked by ESNI.
Conclusions

- 10% websites among Alexa Top 1M are supporting ESNI.
- 84.5% currently censored websites will remain blocked in China even if DNS- and SNI-based censorship are evaded.
- Only 66 websites currently censored in China can be unblocked by ESNI.
- No ESNI-based censorship is detected in our experiment across 14 different areas.
Contacts

Zimo Chai - CS MS/PhD Student
zchai@cs.umass.edu

SPIN Lab, with Amir Houmansadr
https://people.cs.umass.edu/~amir/Research.html

We have released all our probing tools and datasets at http://traces.cs.umass.edu/index.php/Network, to maintain reproducibility and to benefit future research works.
Let’s Enable ESNI Now!

1. Open `about:config` in Firefox
2. Set `network.security.esni.enabled` to `true`
3. Set `network.trr.mode` to `3`
4. Set `network.trr.uri` to `https://1.1.1.1/dns-query`
5. Check if it works: `https://www.cloudflare.com/ssl/encrypted-sni`