Alternative (ab)uses for HTTP Alternative Services

Trishita Tiwari
Ari Trachtenberg
Boston University

This research was partly supported by National Science Foundation, grant CCF-1563753
Outline

1. Background: HTTP
2. Alt-Svc header
3. Attacks w/ Alt-Svc
4. Mitigations
5. Industry response
6. Conclusion
HTTP

- HTTP/1.0 in 1996

- Simple headers:
  - Hostname
  - Referer
  - User-Agent
HTTP

- HTTP expanded:
  - Caching
  - Dynamic content
  - Request multiplexing

- Result = more papers for security researchers 😊
HTTP is as old as me (22 yrs)

Yet hard to introduce secure protocol updates.
Alternative Services (RFC 7838)

- Yet another HTTP header!!
- Allows website to specify equivalent alternate endpoint

Tired senior who needs to finish thesis
Alternative Services (RFC 7838)

https://original.com/

Client browser

original.com
Alternative Services (RFC 7838)

Client browser

https://original.com/

Alt-Svc: alt.com:443

original.com

... HTML content
Alternative Services (RFC 7838)

Client browser

https://original.com/

Alt-Svc: alt.com:443

... HTML content

TLS client hello

alt.com:443

original.com
Alternative Services (RFC 7838)

Client browser

https://original.com/

Alt-Svc: alt.com:443

TLS client hello

TLS Server hello, cert exchange

original.com

alt.com:443

HTML content
Alternative Services (RFC 7838)

Client browser

https://original.com/

Alt-Svc: alt.com:443

... HTML content

TLS client hello

TLS Server hello, cert exchange

Mapping cached if cert valid for original.com

original.com

alt.com:443
Alt-Svc: ‘h2="www.google.com:123"; ma=123456’
Alt-Svc format

Alt-Svc: ‘h2="www.google.com:123"; ma=123456’

Protocol (http/1.1, quic, h2c, ftp, etc.)
Alt-Svc format

Alt-Svc: ‘h2="www.google.com:123"; ma=123456’

Protocol (http/1.1, quic, h2c, ftp, etc.)
Alt-Svc format

Alt-Svc: ‘h2="www.google.com:123"; ma=123456’

- Domain/IP
- Port
- Protocol (http/1.1, quic, h2c, ftp, etc.)
Alt-Svc format

- Domain/IP
- Port
- Protocol (http/1.1, quic, h2c, ftp, etc.)
- Max age (s)

Alt-Svc: ‘h2="www.google.com:123"; ma=123456’
Alt-Svc Uses

- Load balancing
- Client segmentation
- Advertising endpoints with new protocols
Overview of abuse

- Port Scan (CVE 2019-11728)
- DDoS
- Alt-Svc Abuses
- History Exfiltration
- Malware protection bypass
- Tracking
Threat model

- **Case #1:**
  - Attacker controls website(s)

- **Case #2:**
  - Attacker controls website(s)
  - Monitors victim network traffic
    - E.g. Cafe/Airport WiFi
Port-Scan (CVE-2019-11728)

- (Distributed) port scanning (from browser context).

http://evil.com/p1

Alt-Svc: “h2=localhost:25”
Port-Scan (CVE-2019-11728)

- (Distributed) port scanning (from browser context).

http://evil.com/p1
Alt-Svc: “h2=localhost:25”

Browser validates Alt-Svc
<table>
<thead>
<tr>
<th>Closed Port</th>
<th>Open Port</th>
</tr>
</thead>
</table>

Time: 3.1/6
Port-Scan (CVE-2019-11728)

Closed Port

RST

Open Port

Time

3.1/6
Port-Scan (CVE-2019-11728)

Closed Port

- RST

Open Port

- PKT

Time
# Port-Scan (CVE-2019-11728)

<table>
<thead>
<tr>
<th>Closed Port</th>
<th>Open Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>RST</td>
<td>PKT</td>
</tr>
<tr>
<td></td>
<td>PKT</td>
</tr>
</tbody>
</table>

Time: 3.1/6
Port-Scan (CVE-2019-11728)

<table>
<thead>
<tr>
<th>Closed Port</th>
<th>Open Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>RST</td>
<td>PKT</td>
</tr>
<tr>
<td></td>
<td>PKT</td>
</tr>
<tr>
<td></td>
<td>PKT</td>
</tr>
</tbody>
</table>

Time: 3.1/6
Port-Scan (CVE-2019-11728)

<table>
<thead>
<tr>
<th>Closed Port</th>
<th>Open Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>RST</td>
<td>PKT</td>
</tr>
<tr>
<td>RST</td>
<td>PKT</td>
</tr>
<tr>
<td>RST</td>
<td>PKT</td>
</tr>
</tbody>
</table>

Time
Port-Scan (CVE-2019-11728)

Closed Port

- RST

Open Port

- PKT
- PKT
- PKT
- RST

Time
Port-Scan (CVE-2019-11728)

- Closed Port: RST
- Open Port: PKT, PKT, PKT

Time: ?
Port-Scan (CVE-2019-11728)

**Closed Port**
- RST

**Open Port**
- PKT
- PKT
- PKT

Time

3.1/6
Port-Scan (CVE-2019-11728)

Closed Port

- RST

Redirect: http://evil.com/p2
Alt-Svc: “h2=evil2.com:443”

Open Port

- PKT
- PKT
- PKT

Time
Port-Scan (CVE-2019-11728)

Closed Port

- RST

Redirect: http://evil.com/p2
Alt-Svc: “h2=evil2.com:443”

Open Port

- PKT
- PKT
- PKT

Browser connects to new Alt-Svc
Port-Scan (CVE-2019-11728)

Closed Port

- RST

Redirect: http://evil.com/p2
Alt-Svc: “h2=evil2.com:443”

Open Port

- PKT
- PKT
- PKT

Browser connects to new Alt-Svc

Browser DOES NOT connect to new Alt-Svc
Port-Scan consequences

- Distributed port scanning
- Localhost, private networks (behind firewall/NAT)
- TCP ports, some UDP ports
- Attacker identity is not revealed!
Alt-Svc Abuses

- Port Scan (CVE 2019-11728)
- DDoS
- History Exfiltration
- Malware Protection Bypass
- Tracking
Malware protection bypass

Victim browser → www.dangerous.com
Malware protection bypass

Victim browser ➔ www.dangerous.com

Safe browsing
Malware protection bypass

- Blocks first and third party:
  - www.dangerous.com in URL bar
  - `<img src=www.dangerous.com>` in www.example.com
Malware protection bypass

Deceptive site ahead

Attackers on tidsincludedirectory.club may trick you into doing something dangerous like installing software or revealing your personal information (for example, passwords, phone numbers, or credit cards). Learn more

Help improve Safe Browsing by sending some system information and page content to Google. Privacy policy

Details  Back to safety
Malware protection bypass

- www.example.com specifies www.dangerous.com as its Alt-Svc.
- Browser allows content loading from www.dangerous.com!
Malware protection bypass

- www.example.com specifies www.dangerous.com as it’s Alt-Svc.

- Browser allows content loading from www.dangerous.com!
Malware protection bypass

- www.example.com specifies www.dangerous.com as its Alt-Svc.
- Browser allows content loading from www.dangerous.com!
Two-faced content

Original
www.example.com

Alt-Svc
www.dangerous.com

Automated scanners check

User browser loads
Two-faced content

Original
www.example.com

Alt-Svc
www.dangerous.com

Automated scanners check

User browser loads

Vulnerable: URLVoid, VirusTotal, Sucuri, IPVoid
Alt-Svc Abuses

- Port Scan (CVE 2019-11728)
- DDoS
- History Exfiltration
- Malware protection bypass
- Tracking
Many clients connect to victim Alt-Svc endpoint: DDoS!

- Long timeouts
- Bandwidth Exhaustion
DDoS: Long timeouts

Attacker

Victim Server

Browser
DDoS: Long timeouts

Attacker → Browser → Long lasting connections → Victim Server
DDoS: Long timeouts

Attacker → Browser → Victim Server

Long lasting connections
DDoS: Long timeouts

Attacker → Long lasting connections → Victim Server

Browser
DDoS: Long timeouts

- Attacker
- Long lasting connections
- Victim Server
- Browser
DDoS: Long timeouts

- FTP, SMTP, etc. servers

Diagram:
- Attacker
- Browser
- Long lasting connections
- RIP
DDoS: Bandwidth exhaustion

Attacker

Browser

Victim Server
DDoS: Bandwidth exhaustion
DDoS: Bandwidth exhaustion

Attacker

Small TLS client
hello Packets

Victim Server

Browser
DDoS: Bandwidth exhaustion

Attacker

Small TLS client
hello Packets

Victim Server

Browser
DDoS: Bandwidth exhaustion

Attacker → Small TLS client
   hello Packets → Victim Server

Browser
DDoS: Bandwidth exhaustion

- **Attacker**
- Large TLS server certs
- **Victim Server**
- **Browser**
DDoS: Bandwidth exhaustion

- Attacker
- Large TLS server certs
- Victim Server
- Browser
DDoS: Bandwidth exhaustion

- Attacker
- Large TLS server certs
- Victim Server
- Browser
DDoS: Bandwidth exhaustion

Attacker

Browser

Large TLS server certs

Victim Server
• SMTP, HTTPS, etc. (any TLS speaking servers).

**DDoS: Bandwidth exhaustion**

- Attacker
- Large TLS server certs
- RIP
- Browser
Alt-Svc Abuses

- Port Scan (CVE 2019-11728)
- DDoS
- History Exfiltration
- Malware protection bypass
- Tracking
• Alt-Svc mapping is cached by browser.

• Specify unique value for each user to track.

• Works 1st and 3rd party, bypassing known tracking blockers.
Port Scan (CVE 2019-11728)

Alt-Svc Abuses

DDoS

History Exfiltration

Malware protection bypass

Tracking
History exfiltration

- Captive WiFi Portal
- Restaurants, coffee shops, hotels
History exfiltration

ISP 1

Victim

Did Victim visit illegal.com?
History exfiltration

- Victim
- ISP 1
- `<iframe src=illegal.com>`
- `wifi.login.com`
History exfiltration

Victim → ISP 1

<iframe src=illegal.com>

ISP 1 → wifi.login.com

ISP 1 → illegal.com
History exfiltration

Victim

<iframe src=illegal.com>

ISP 1

wifi.login.com

Unvisited

illegal.com

ISP 1
History exfiltration

Victim

<iframe src=illegal.com>

ISP 1

alt.illegal.com

ISP 1

wifi.login.com
History exfiltration

- Victim
- ISP 1
- <iframe src=illegal.com>
- wifi.login.com
- alt.illegal.com
- Visited
- ISP 1
Mitigations

- **Port-Scan, DDoS:**
  Block sensitive ports

- **Safe Browsing:**
  Alt-Svc domain check

- **Tracking, History Exfiltration:**
  Isolate Alt-Svc cache
<table>
<thead>
<tr>
<th>Malware protection bypass</th>
<th>5/6</th>
<th>5/6</th>
<th>5/6</th>
<th>5/6</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fixed</td>
<td>5/6</td>
<td>5/6</td>
<td>5/6</td>
<td>5/6</td>
</tr>
<tr>
<td>In process</td>
<td>5/6</td>
<td>5/6</td>
<td>5/6</td>
<td>5/6</td>
</tr>
<tr>
<td>Unpatched</td>
<td>5/6</td>
<td>5/6</td>
<td>5/6</td>
<td>5/6</td>
</tr>
<tr>
<td>Unaffected</td>
<td>5/6</td>
<td>5/6</td>
<td>5/6</td>
<td>5/6</td>
</tr>
</tbody>
</table>

**Industry response**

<table>
<thead>
<tr>
<th>Port-Scan</th>
<th>Firefox</th>
<th>TOR</th>
<th>Chrome</th>
<th>Brave</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>DDoS</th>
<th>Firefox</th>
<th>TOR</th>
<th>Chrome</th>
<th>Brave</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Tracking</th>
<th>Firefox</th>
<th>TOR</th>
<th>Chrome</th>
<th>Brave</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>History exfiltration</th>
<th>Firefox</th>
<th>TOR</th>
<th>Chrome</th>
<th>Brave</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Conclusion

- New but widely adopted Alt-Svc is vulnerable
- 5 attacks(!), despite:
  - Maturity of HTTP
  - Highly competent browser developers
- Securing is not easy!
References

- Icons made by Smashicons from Flaticon is licensed by CC 3.0 BY
- Icons made by Freepik from Flaticon is licensed by CC 3.0 BY
- Http Icon #286170 made by Icon Library
Questions?

Don't drink...

...And Alt-Svc