IETF 97 HTTPbis Working Group
Tuesday, November 15, 2016

Experiences with Alt-Svc for HTTP Opportunistic Security

Nick Sullivan

History

- draft-ietf-httpbis-http2-encryption
- A way to use HTTP over TLS without validating certificate
- Enables HTTP/2 for non-HTTPS sites
- Different from HTTPS, no secure context
  - Browser treats OppEnc HTTP as HTTP
  - HTTPS requires subresources to also use the HTTPS scheme

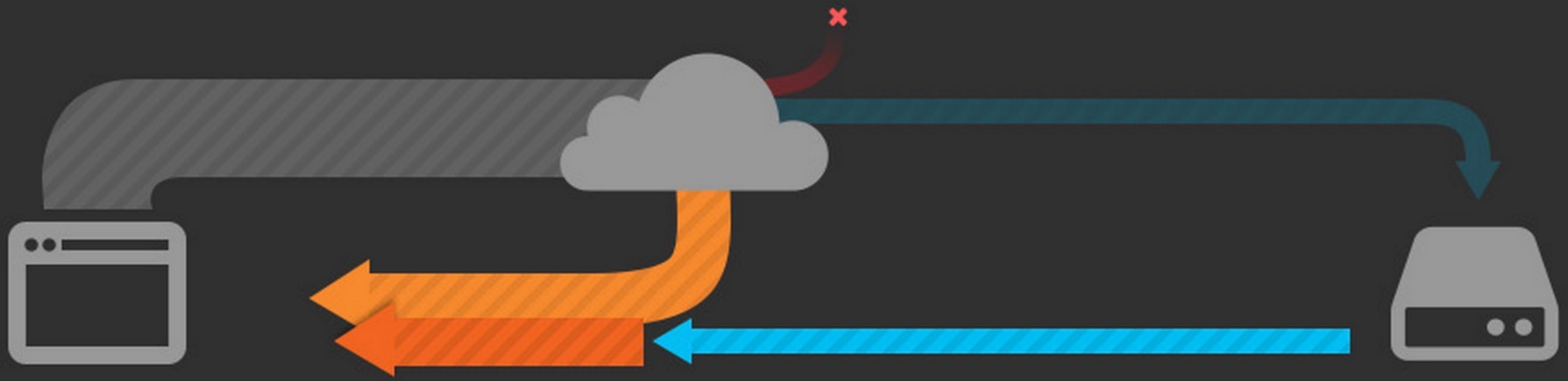
Ecosystem changes

- Certificates are no longer the bottleneck
  - Let’s Encrypt
  - Cloudflare’s Universal SSL
- No widespread solution to mixed content
- Proposed changes by to enforce certificate validation
  - Opportunistic Encryption -> Opportunistic Security

Cloudflare overview

- 4 million+ Free customers of all kinds
  - Static sites, Wordpress, Drupal, etc.
  - Large number of sites without active content maintenance, legacy HTML
- Paid customers
  - Pro sites (20$/month) ~100s of thousands
  - Business + Enterprise (200$/month) ~10s of thousands

Cloudflare Reverse Proxy



Encryption Week: September 2016

- Improve the security and performance of Cloudflare customers automatically
  - TLS 1.3: improve security for HTTPS sites
  - Automatic HTTPS rewrites (enable HTTPS for sites with fixable mixed content)
  - Opportunistic Encryption with valid certificates by default
- Enabled for free/pro sites by default

Opportunistic Security Headers

```
Alt-Svc: h2=":443"; ma=60
```

http://enabledzone.org/.well-known/http-opportunistic (since changed in draft)

```
{
  "http://enabledzone.org": {
    "tls-ports": [443],
  }
}
```

CLOUDFLARE

Results

- Implemented in part of tiered reverse proxy architecture (nginx:443 → nginx:80 → upstream:80)
- Initial attempt relied on the **`alt-used`** header to distinguish OE vs HTTPS, this failed on sites when in privacy mode
- Custom code changes required for nginx/OpenResty to expose the scheme pseudo-header and choose http:80 upstream instead of https:443
- 25-75k rps encrypted with opportunistic encryption

Tiny sample from Free/Pro October 24

- 143919 requests made by OE-supporting versions of Firefox
- 29814 (21%) were HTTPS
- 37591 (26%) were upgraded to HTTP over TLS (HTTP/2 or SPDY) using OE
- 76514 (53%) were plaintext HTTP:
  - Of the top 100 hosts, 6011 out of 28214 requests (21%) could have been upgraded using OE (Alt-Svc header served)
  - Not all hosts support OE (e.g. no SSL cert for subdomains); the most popular host doesn't, and at least 7859 requests do not support it

Outcomes

- When OE is enabled, a large number of requests get encrypted
- Many zones don’t benefit because they disabled SSL or disabled OE explicitly; we could encourage use of the feature and double uptake
- More investigation needed to see if increasing OE cache TTLs improve encryption rate
- Possible that Firefox could use OE more aggressively on the first page load and fetch linked resources over TLS (see network inspector in devtools)

Conclusions

- Effective tool for reducing plaintext
- More secure, more performant baseline for HTTP
- Especially useful to enable on behalf of sites
- Generally effective against bulk surveillance, not directed attacks
- Customers generally didn’t notice
- Incentives for moving sites HTTPS remain intact
  - No customers used this as an alternative to fixing fixable mixed content

IETF 97 HTTPbis Working Group
Tuesday, November 15, 2016

Experiences with Alt-Svc for HTTP Opportunistic Security

Nick Sullivan