RSAConference2016

San Francisco | February 29 – March 4 | Moscone Center

Connect to Protect

SESSION ID: ASD-R02

Understanding HTTP/2

Nathan LaFollette

Managing Consultant
Trustwave SpiderLabs
@httphacker

#RSAC

Agenda

- Brief History of HTTP
- The Good, The Bad, The Ugly
- Supported Configurations
- Final Thoughts

History of HTTP – The Protocol Evolution

- 1989 – WWW
- 1991 – HTTP 0.9
- 1996 – HTTP 1.0
- 1997 – HTTP 1.1
- 2012 – HTTP 1.1 bis?
- 2012 – SPDY v1
- 2012-2015 – SPDY v2, v3, v3.1, v4 alpha3
- 2015 – HTTP/2

Why a new version?

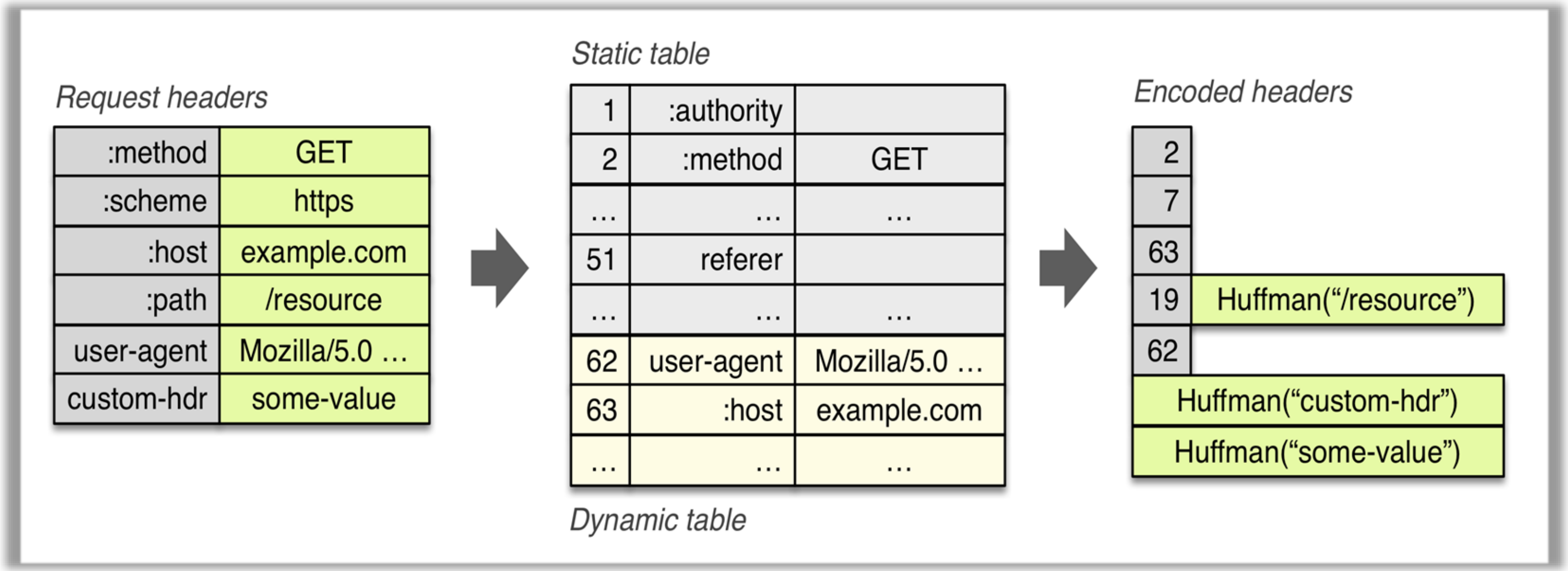
- As the web advances, we struggle to 'keep up'
- Less header tampering as with HTTP/1.1
- Added and required encryption
- QoS for the web
- Scalability for Modern Applications
- Job Security for the industry ☺

The Good – What comes with it?

- Comes with new Goodness
  - Compression
  - Server or Site Pushing
  - Prioritization
  - Multiplexing
- Defense Mechanism
- Increases SEO weight
- Compliments CDNs and WAN Acceleration

Compression

- HPACK – Dedicated Header Compression


Request headers

:method	GET
:scheme	https
:host	example.com
:path	/resource
user-agent	Mozilla/5.0 …
custom-hdr	some-value

Static table

1	:authority	
2	:method	GET
…	…	…
51	referer	
…	…	…
62	user-agent	Mozilla/5.0 …
63	:host	example.com
…	…	…

Dynamic table

Encoded headers

2	
7	
63	
19	Huffman("/resource")
62	
Huffman("custom-hdr")	
Huffman("some-value")	

Image Courtesy of O'Reilly Media

Server Pushing

- Push Promising

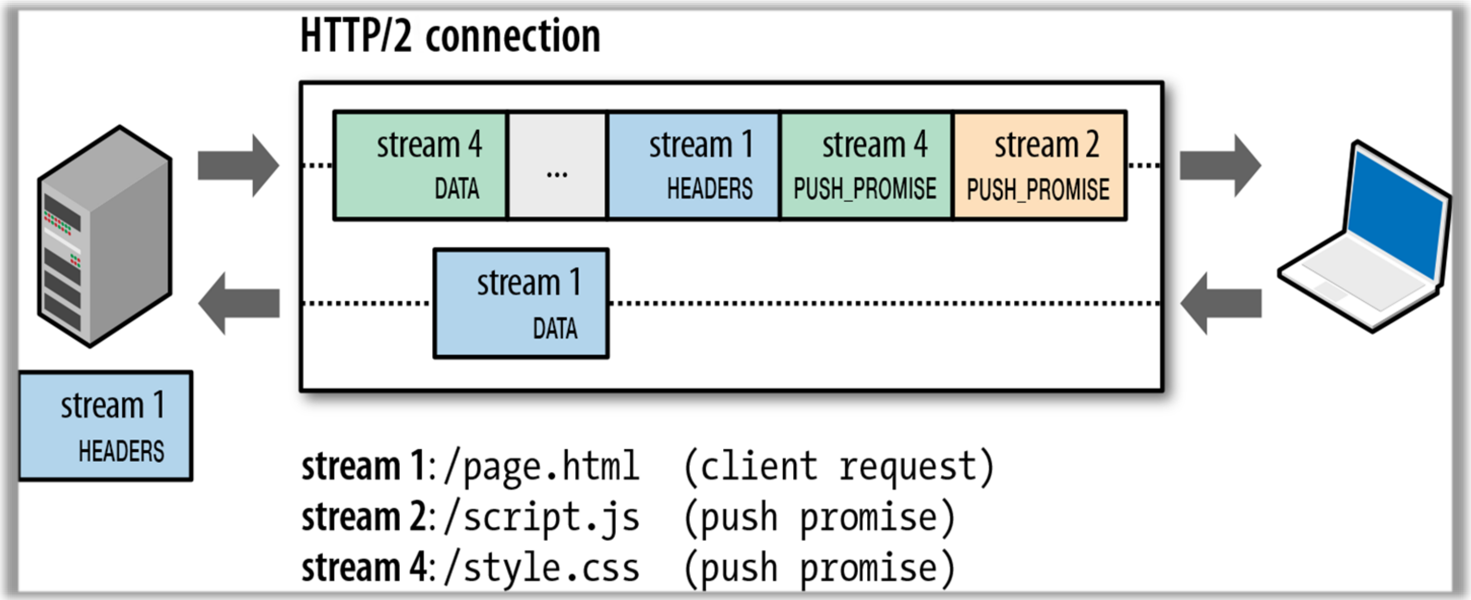


Image Courtesy of O'Reilly Media

Prioritization

- Prioritizing Frames

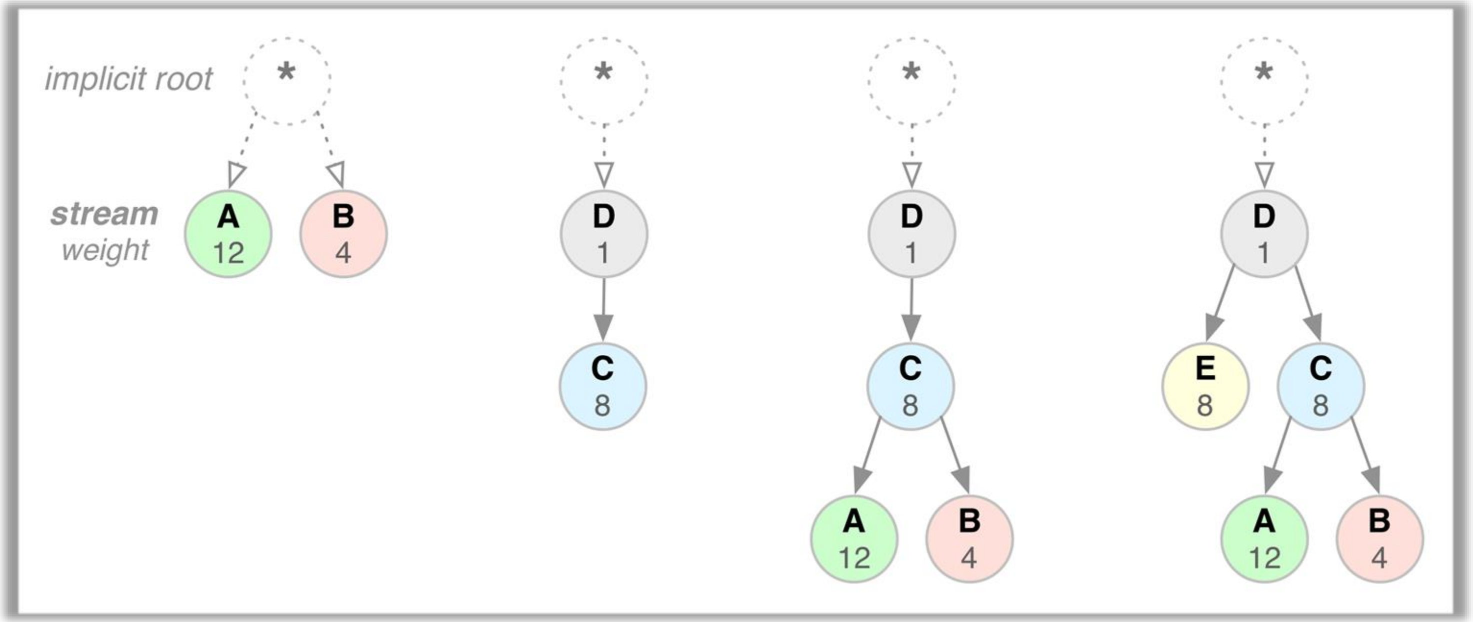


Image Courtesy of O'Reilly Media

Multiplexing

- A Single TCP Connection

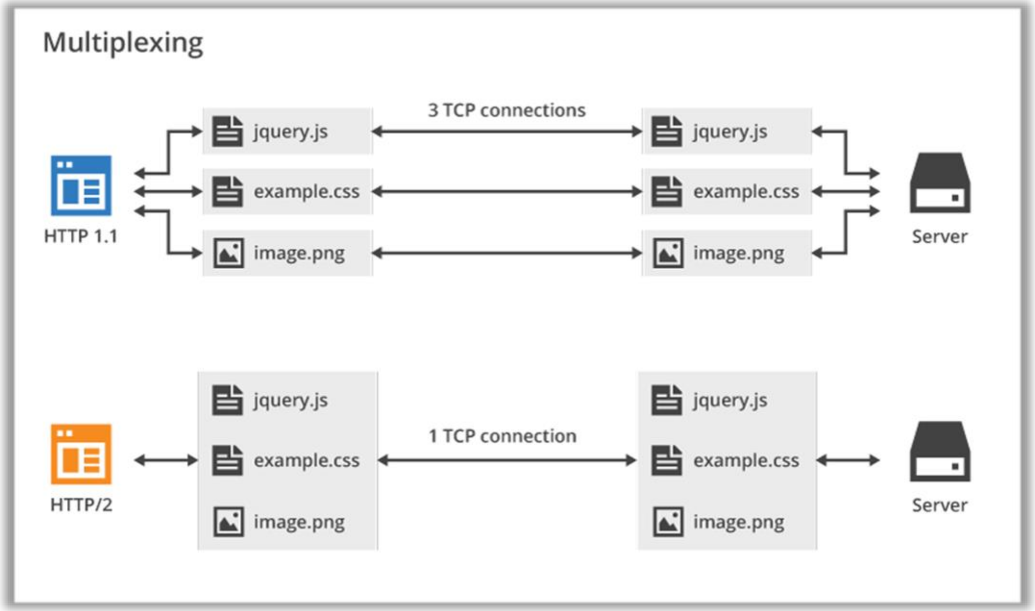


Image Courtesy of CloudFlare

Why not just enhance SPDY?

- SPDY is susceptible to CRIME, a byproduct of Gzip/deflate header compression
- No cryptography cipher strength requirements
- SPDY only has Single-Host Multiplexing
- Not fast enough encrypted connections – uses NPN, not ALPN
- Prioritization less flexible to proxies

The Bad and Ugly – What makes it hurt?

- User experience and compatibility
- Lack of developmental tools
- Reimplementation and architectural considerations
- No good security testing tools
- Unknown issues with existing technologies

Supported Configurations

- Server Support
  - Apache 2.4.12 via mod_h2 & Apache Traffic Server
  - Citrix NetScaler
  - F5 BIG-IP Local Traffic Manager 11.6
  - h2o
  - Jetty 9.3
  - LiteSpeed Web Server 5.0
  - Microsoft IIS w/Windows 10 & Windows Server 2016
  - Nginx 1.9.5
  - OpenLiteSpeed 1.3.11 and 1.4.8
  - Proxygen
  - Wildfly 9

Supported Configurations

- Content Delivery Network Support
  - Akamai Edge Servers
  - CDN77
  - CloudFlare
  - Imperva Incapsula CDN
  - KeyCDN

Support Configurations

- Traditional Browser Support
  - Chrome (Supports only over TLS)
  - Firefox (Supports only over TLS)
  - Opera
  - Microsoft Edge
  - Microsoft Internet Explorer v11 (Partial)
  - Safari v9.x (Partial)

Support Configurations

- Mobile Browser Support
  - Chrome for Android (Supports only over TLS)
  - Safari for iOS v9.2/9.3

Configuration Considerations

- Server's that were easy to setup in my testing…

H2O	(https://github.com/h2o/h2o)
Caddy Server	(https://caddyserver.com/)
Microsoft IIS	(http://blogs.iis.net/davidso/http2)
Apache	(https://github.com/icing/mod_h2)
Nginx	(https://www.nginx.com/blog/)

Validating HTTP/2

- Browser Indicators
  - Extensions (My Favorite → HTTP/2 & SPDY Indicator)
  - Debuggers and Developer Views
- Command Line Tools (http2fuzz)
- Load Testing
- Packet Snooping

Final Thoughts - What Next?

- Next week you should:
  - Identify commonly used websites and their HTTP/2 implementation status
- In the first three months following this presentation you should:
  - Configure a Web Server for HTTP/2
  - Configure a CDN to work with your HTTP/2 Server
- Within six months you should:
  - Deploy Web and Mobile Applications utilizing advanced features of HTTP/2, like Prioritization and Server Pushing

RSA Conference2016

San Francisco | February 29 – March 4 | Moscone Center

Connect to Protect

SESSION ID: ASD-R02

Understanding HTTP/2

Nathan LaFollette

Managing Consultant
Trustwave SpiderLabs
@httphacker

#RSAC