

# HTTP/2.0, NSA and/or Web performance



Poul-Henning Kamp

phk@FreeBSD.org

phk@Varnish.org

@bsdphk

\$ who am i

Author of md5crypt

Author of an awful lot of FreeBSD kernel

Author of Varnish HTTP cache

Author of a lot of other code

Trainee Grumpy Old Man

0x30 years old, 040 years with computers

# HTTP/1.1 client performance

- (\* Time to DNS resolution)
- (\* Time to validate DNSSEC)
- \* Time to TCP SYN+ACK
- (\* Time to negotiate TLS)
- \* Time to status code
- \* Time to first body byte
- \* "TTT" } "multimedia industry" metrics
- \* "TTA" }
- \* Time to last body byte

...it's all about instant gratification.

# HTTP/2.0 client performance

- (\* Time to DNS resolution)
- (\* Time to validate DNSSEC)
- \* Time to TCP SYN+ACK <== Fewer (mux)
- \* Time to negotiate TLS <== Mandatory
- \* Time to status code <== Faster (mux, compr)
- \* Time to first body byte
- \* "TTT" } "multimedia industry" metrics
- \* "TTA" }
- \* Time to last body byte

...it's all about instant gratification.

# HTTP/1.1 server performance

- \* Connections per second
- \* Client identifications per second (GeoIP etc.)
- (\* TLS negotiations per second)
- \* Requests per second
- \* Cheap request-ratio (IMS, cache hits &c)
- \* Bytes per second
- \* Idle connections
- \* DoS attacks per day
- \* DoS SYN/sec
- \* DoS bytes/sec
- \* Site availability %
- \* Cost of operation

# HTTP/2.0 server performance

- \* Connections per second <== Lower
- \* Client identifications per second (GeoIP etc.)
- \* TLS negotiations per second <== Mandatory
- \* Requests per second
- \* Cheap request-ratio (IMS, cache hits &c)
- \* Bytes per second
- \* Idle connections <== Lower
- \* DoS attacks per day
- \* DoS SYN/sec
- \* DoS bytes/sec
- \* Site availability %
- \* Cost of operation <== Higher
- \* Less client-side proxying
- \* Big Per Connection State
- \* Higher CPU load
- \* Bigger DoS surface

# HTTP/2.0 – a political protocol



# IETF politics

Mike Belsche @Google made SPDY

\$BIGSITE + \$OWNBROWSER = \$WE\_DONT\_CARE\_ABOUT\_IETF ?

HTTPbis WG had (almost!) finished multi-year project to "clarify" HTTP/1.1

Before 1 RFC @ 9859 lines

After 11 RFCs @ 19745 lines

Sudden requirement for "HTTP/2.0" protocol

Accelerated schedule mean that

"SPDY was only realistic proposal"



# HTTP/2.0 political factions

## \$BIGGUYS

- Hates telcos for meddling in their traffic
- Want to track users all over the web
- Makes money selling peoples privacy

## \$TELCOS

- Wants to use client side proxies
  - Bandwidth conservation
  - Add injection on "Free Internet"
- Traffic inspection (sell info)
- Traffic "shaping" (extort NetFlix)

## NSA

- Wants a clear-text copy of all comms.

# HTTP/2.0 political factions

## "Multimedia business"

- Fast cheap "multimedia" delivery
- Doesn't give a shit about anything but money

## \$BIGNEWS

- Fast cheap delivery of content and adds

## Legal

- Traffic inspection w/ per-site client proxy
  - Child protection & Anti-smut filtering
  - Prison Inmate surveillance
  - SOX compliance
  - Other flight recorder legal req's.

# HTTP/2.0 political factions

## Free Software developers

- Apache
- Varnish
- Nginx
- Jetty

Each beholden to their users req's.

## Tied software developers

- All the browsers

Each beholden to their puppet masters

# Crypto mumbo-jumbo

## Authentication

- > You know who you're talking to
- > Requires trusted 3rd. party ("CA")

## Confidentiality

- > Nobody can understand your conversation.

## Privacy

- > Only the communicating parties know.

Privacy = Authentication + Confidentiality

# The crypto threats

## Passive surveillance

- What NSA does to everybody
- Only records traffic, doesn't send packets.
- Defeated by confidentiality via crypto

## Man-In-The-Middle

- Modifies traffic
  - Insert ads (telcos, hotels)
  - Pretend to be somebody (Police, criminals)
- Inspects traffic
  - SOX, flight recorders
  - Smut filters (Blocks/replaces content)
- Defeated by privacy  
(= confidentiality + authentication.)

# Authentication in practice

”Mostly works”

- \* Bogus root-CA's
  - China State Railroads
  - Mobile carriers
  - Corporate filtering proxies
- \* Real CA's are bogus too
  - At least 9 CA in Firefox default list are untrustworthy.

No alternative to trusted 3rd. party.

-> Who do you trust ?

# Authentication w/DNSSEC/DANE

Replaces CA's with IANA/TLD admins.

- > same result: Mostly works.

- > Possibly cheaper.

# Confidentiality

Can be done with self-signed certs

Would be really bad news for NSA

Browsers treats SSC as radioactive waste

What a coincidence...

Not!



# HTTP/2.0 Status right now

\$BIGGUYS don't want proxies in their traffic

-> Mandatory TLS

(Exception: IE will do HTTP/2.0 plaintext)

HTTP/2.0 is fatter than HTTP/1.0

HTTP/2.0 offers multiplexing/pipelining

Shitty protocol design handwork (my opinion)

Nobody has published server side benchmarks.

# What happens next ?

HTTP/2.0 draft on the way to IETF "Last Call"

- > p=0.9 Rubber stamped
- > p=0.09 Derailed for political reasons
- > p=0.01 Stopped because it is crap

If HTTP/2.0 ratified:

- > Will be adopted by \$BIGGUYS
- > Supports their political agenda

What about the rest of the web ?

- > What is the cost ?
- > Better/worse performance ?
- > Middleware&platform support ?

# What happens after "TLS everywhere"?

Does NSA roll over, play dead ?

Does NSA derail HTTP/2.0 ?

- > Like self-signed-certs ?

- > Like broken-by-design crypto-algs ?

Or will privacy simply be outlawed ?

- > Certificate escrow ?

- > Mandatory weak algorithms ?

# Privacy is a political problem

Cryptography helps but cannot solve the problem.

Hint:

Governments have police, jails and armies  
IETF does not.

Talk to your politician

Elect better politicians

Become a better politician yourself