A cheesy look at HTTP

- from the middle of the sandwich

Poul-Henning Kamp

phk@FreeBSD.org

phk@Varnish.org

@bsdphk

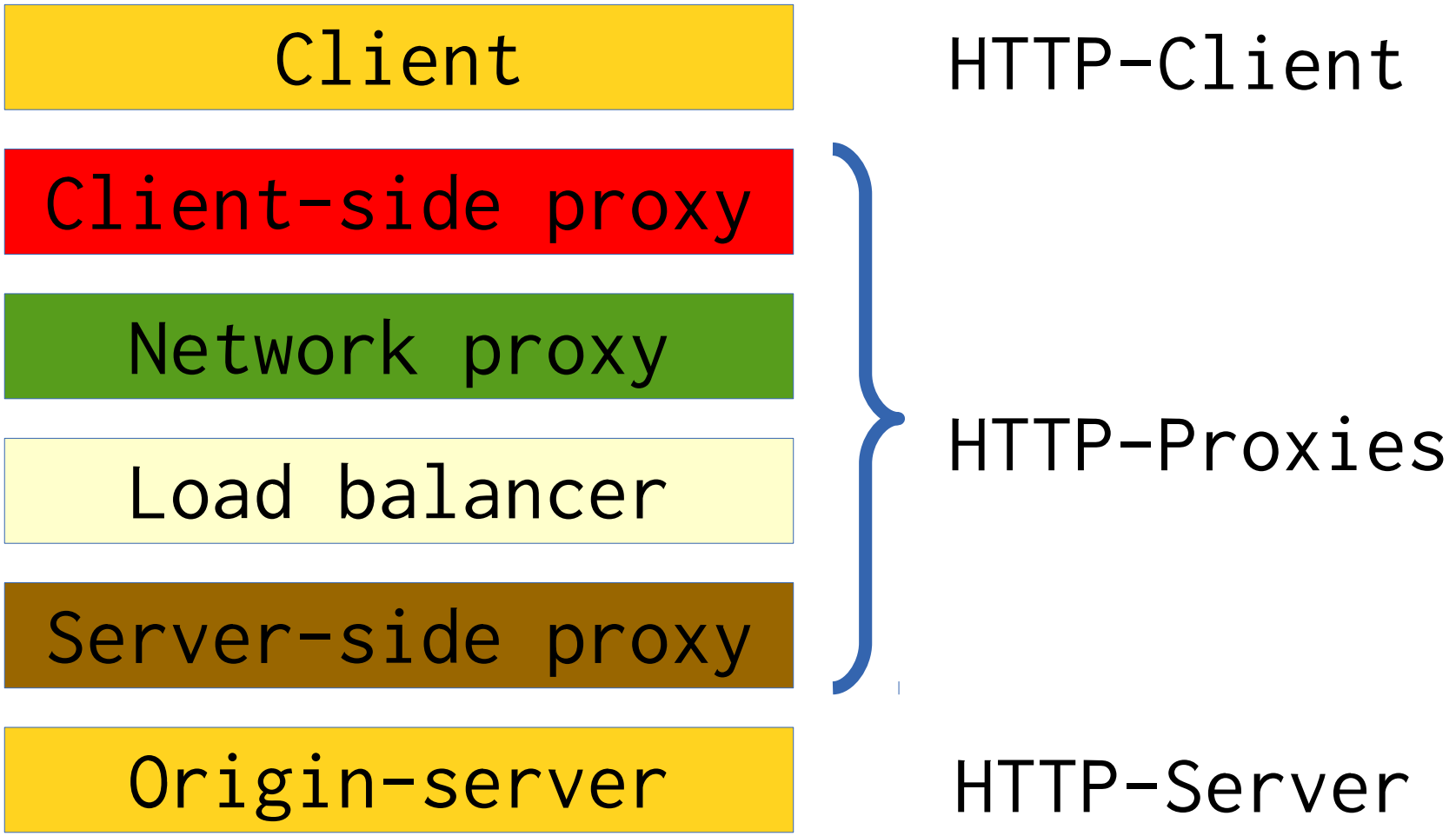
$ finger phk

Poul-Henning Kamp, Self-employed, @.dk

36 years of Computers
32 years of UNIX
30 years of Internet
22 years of FreeBSD
 9 years of Varnish HTTP cache

Bikeshed.org — Read it.
NTP @ nanosecond level
Jails — imperfect virtualization for the win
MD5crypt — All your passwords were belong to me
phkmalloc — 1st paranoid **and** efficient malloc
ESO/ELT adaptive optics on COTS PCs
Hipster before it was hip to be a hipster

The HTTP sandwich



Dictionary definition of Proxy

1 : The agency, function, or office of a deputy who acts as a substitute for another

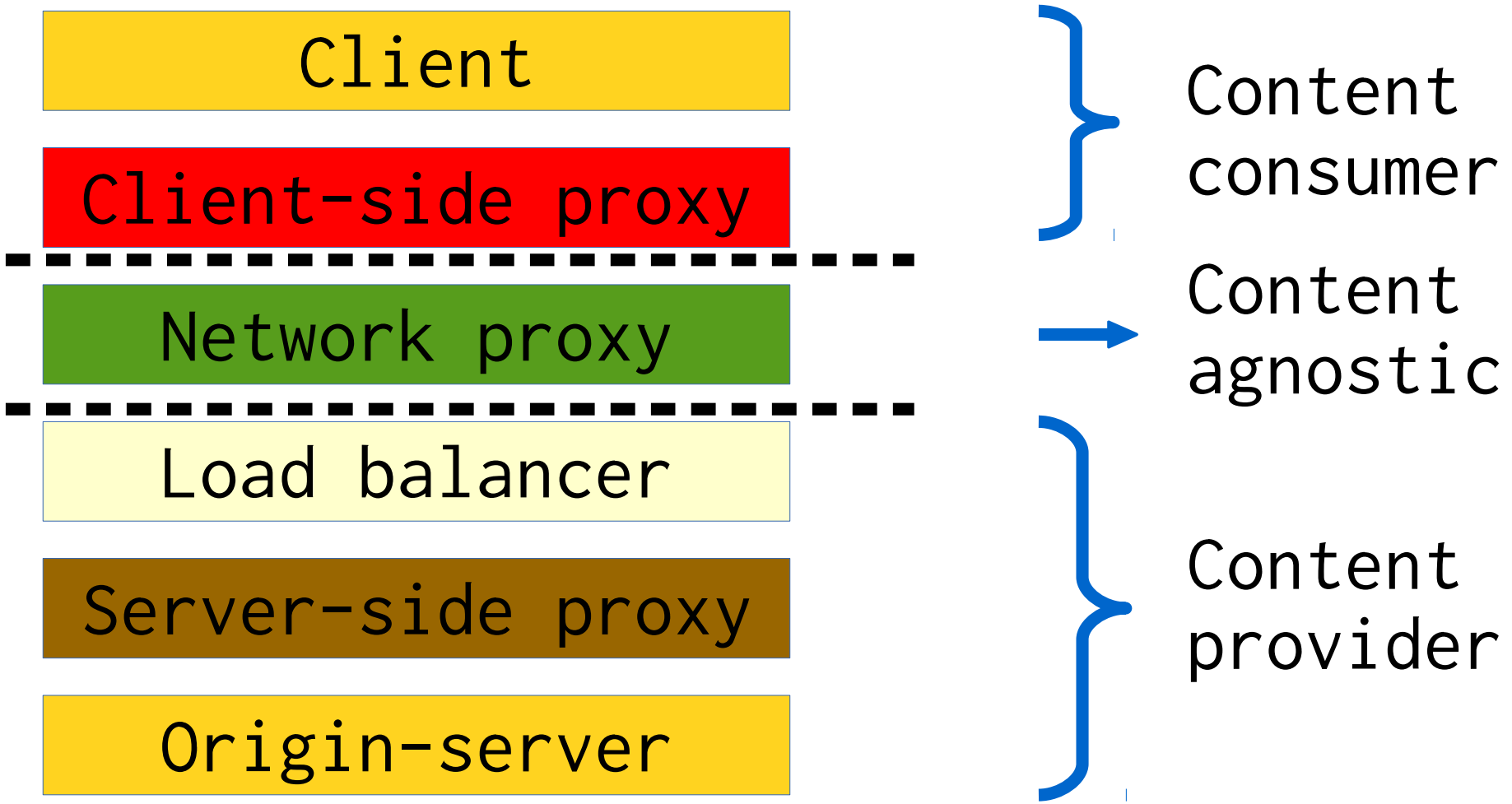
2 a : Authority or power to act for another

b : A document giving such authority; specifically: A power of attorney authorizing a specified person to vote corporate stock

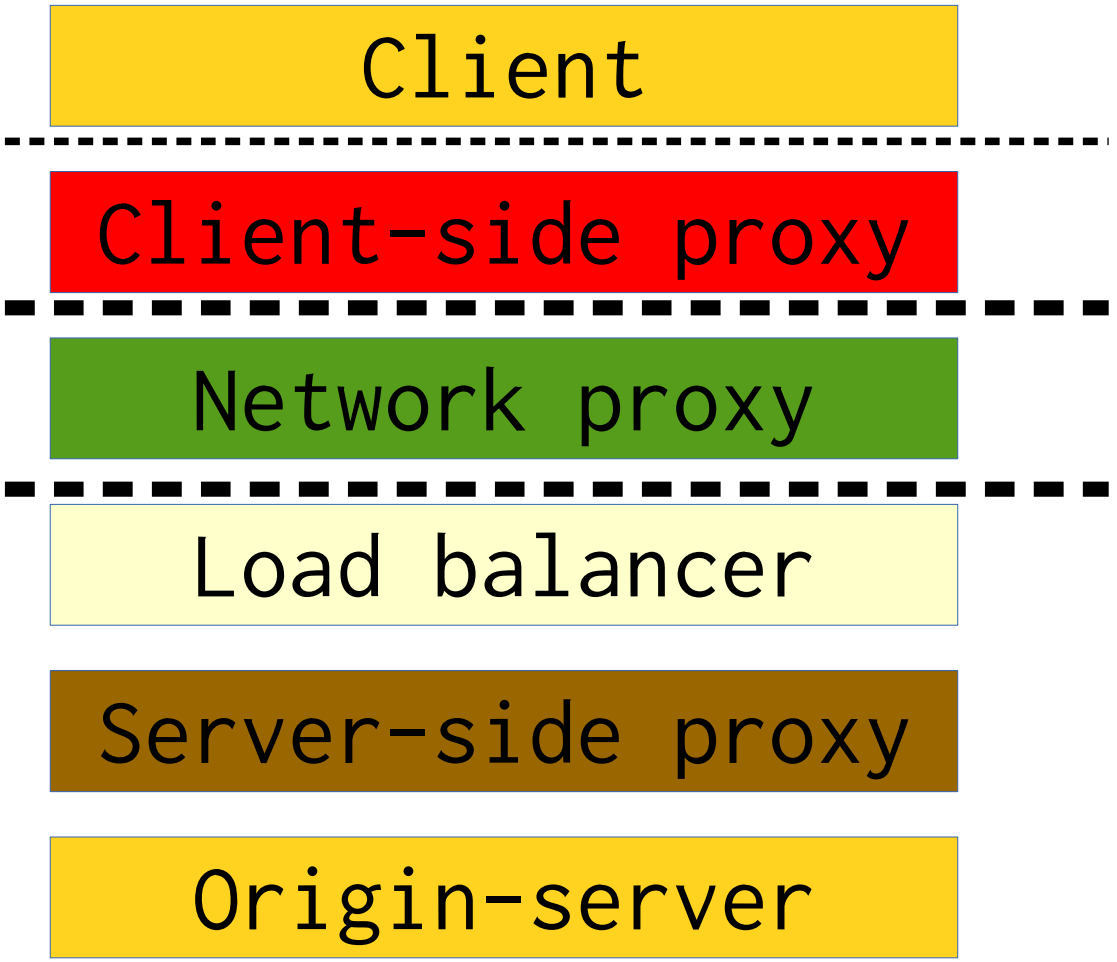
3 : A person authorized to act for another

aka: Man-in-The-Middle

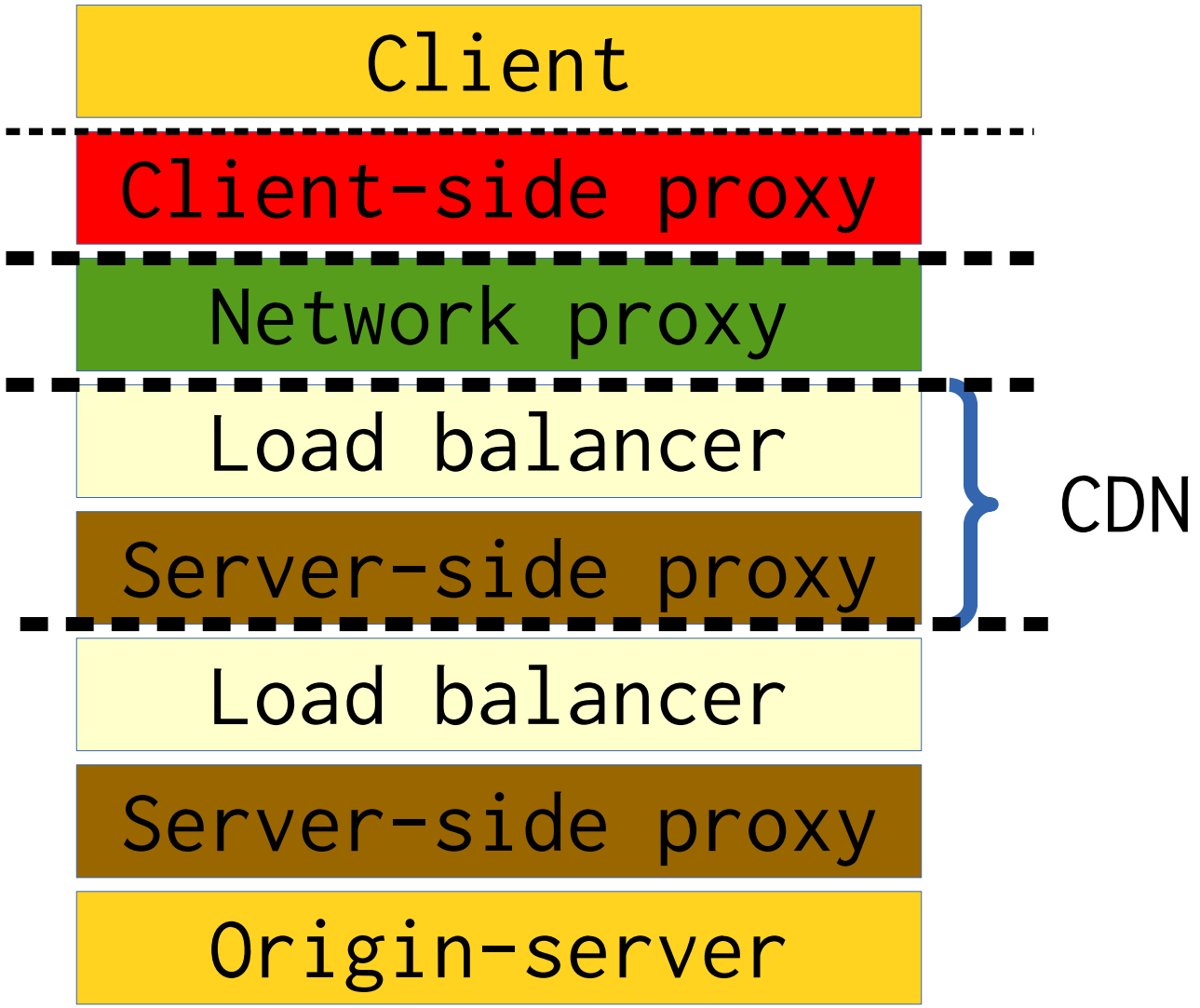
Admin domains, RFC view



Admin domains, real world



The HTTP double sandwich



Who are the Good Guys ?

A) in Balkan _____ (5 pts)

B) in Middle East _____ (10 pts)

C) in HTTP _____ (50 pts)

Client-side proxies, Good or Bad ?

Good:

- Performance gain (caching)
- SOX-compliance recording (MiTM)
- Smut-filters in preschool (MiTM)

Bad:

- Spying
- MiTM attacks

Network proxies, Good or Bad ?

Good:

- Bandwidth / Routing / Latency optimizations
- Emergency Traffic Management
- Law Enforcement (MiTM)

Bad:

- Spying
- MiTM attacks
- Abuse of Monopoly or Market Power

Server side, Good or Bad ?

N/A:

Bad servers cannot cause harm alone
DNS/Net-/Client-proxy collusion req'd.

Badness relates only to their conduct
- not to their HTTP role

Aspects of proxies

Mandated/Legal/Dubious/Illegal:
  What do the applicable laws say ?

Voluntary/Forced:
  Is the client free to use/not use the proxy ?

Hidden:
  Is the client informed about the proxy ?

Tamper:
  Does the proxy tamper with the traffic ?

Spying:
  Does the proxy have sideeffects ?

”Good” proxies:

Legal & Voluntary:
  Cache
  Content filtering
  Anonymity

Legal, Forced, (tampering?) & Spying:
  Parental Controls, smut filters

Mandatory, Forced, Hidden & Spying:
  Court approved crime investigation

Mandatory, Forced & Spying:
  Legal req't: SOX, Prisons, ATC, 911

”Good” proxies:

IETF and which army ?

Legal & Voluntary:
  Cache
  Content filtering
  Anonymity

Legal, Forced, (tampering?) & Spying:
  Parental Controls

Mandatory, Forced, Hidden & Spying:
  Court approved crime investigation

Mandatory, Forced & Spying:
  Legal req't: SOX, Prisons, ATC, 911

”Bad” proxies:

Illegal, Forced, Hidden, Tampering & Spying:

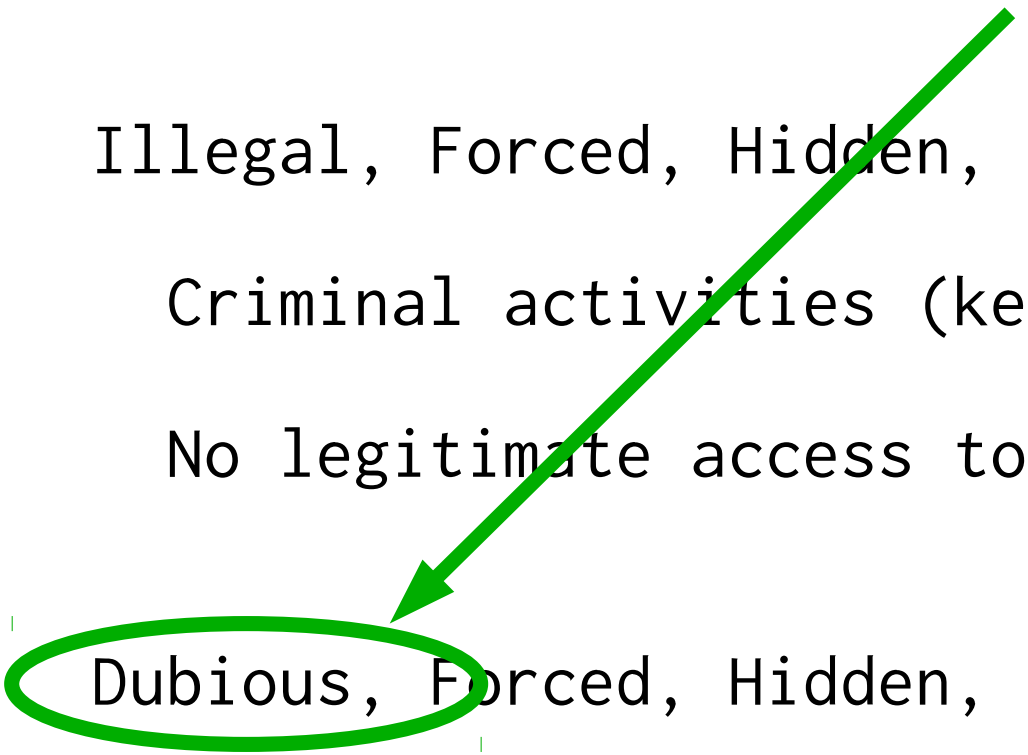
- Criminal activities (key-logging, mitm etc.)
- No legitimate access to traffic -> Illegal

Dubious, Forced, Hidden, Tampering (& Spying ?):

- Ad substitution / Traffic hi-jack / snooping
- Legit access to traffic (ie: ISP) -> Dubious

”Bad” proxies:

Network Neutrality
FCC Title II reg



Illegal, Forced, Hidden, Tampering & Spying:

Criminal activities (key-logging, mitm etc.)

No legitimate access to traffic -> Illegal

Dubious, Forced, Hidden, Tampering (& Spying ?):

Ad substitution / Traffic hi-jack / snooping

Legit access to traffic (ie: ISP) -> Dubious

What about Human Rights and Spying ?

$Spy inside $Jurisdiction:
- Human rights issue
- Has nothing to do with protocol
- Fix it by voting smart(er)
- Sue the bastards in court of law

$Spy outside $Jurisdiction:
- International law (Aka: No law)
- No Fix
- No Justice
- Crypto/OPSEC can harden targets

SSL-everywhere is politically unwise

Prevents legally mandated MiTM

Makes legal and desirable MiTM impossible
- No parental controls is political suicide

Forces other side to use bigger hammer

* Trojan CAs
* Key Escrow
* Short keys
* Crypto ban

Net result: Much less security everywhere

The 4096 bit political question

Q: How to:
    Enable criminal investigations
  and
    Prevent international spying

A: Key Escrow or Trojan CA

Likely SSL-everywhere result:

National Security Law (INTERPOL template):

> All Elbonian persons, companies and domains, SHALL use certs issued by ELBONIA-STATE-CA.
>
> Criminal investigations may obtain necessary cert copies from ELBONIA-CA via court order.
>
> ISP can be ordered by court to assist in criminal investigations.

Privacy [ai]s a human rights issue

HR can only be won via a political process

No post-Snowden national election has had privacy as significant theme anywhere in the world

No major political party has privacy as priority

No significant IT person has been elected

Privacy as an IT issue

No consensus in IT-world about privacy

CIO literature is very anti-privacy

About 250k-500k well paid global jobs in spying

Anti-privacy is BIG business

Click here to follow us: 

Tecnical fixes to political problems

History, learn or repeat:

Technological workarounds for policy
benefit only the ruling class & the intelligencia.

Two-edged sword: Possession of tech workaround
is self incriminating evidence when convenient.

Technology becomes a tool for refeudalisation

And this technical fix sucks!

Mean Time To Notice Broken Crypto: Years

All software has too many bugs

By nature of how we do make:
  1 line in every 1000 is buggy

Intentionally:
  ”Customer support access”
  Commercial exploitation
  Government Infiltration
    (FOSDEM video: ”Operation Orchestra”)

How to win a right to privacy

Get involved in politics

Elect better politicians

Become a better politician yourself

Human Rights is not a spectator sport

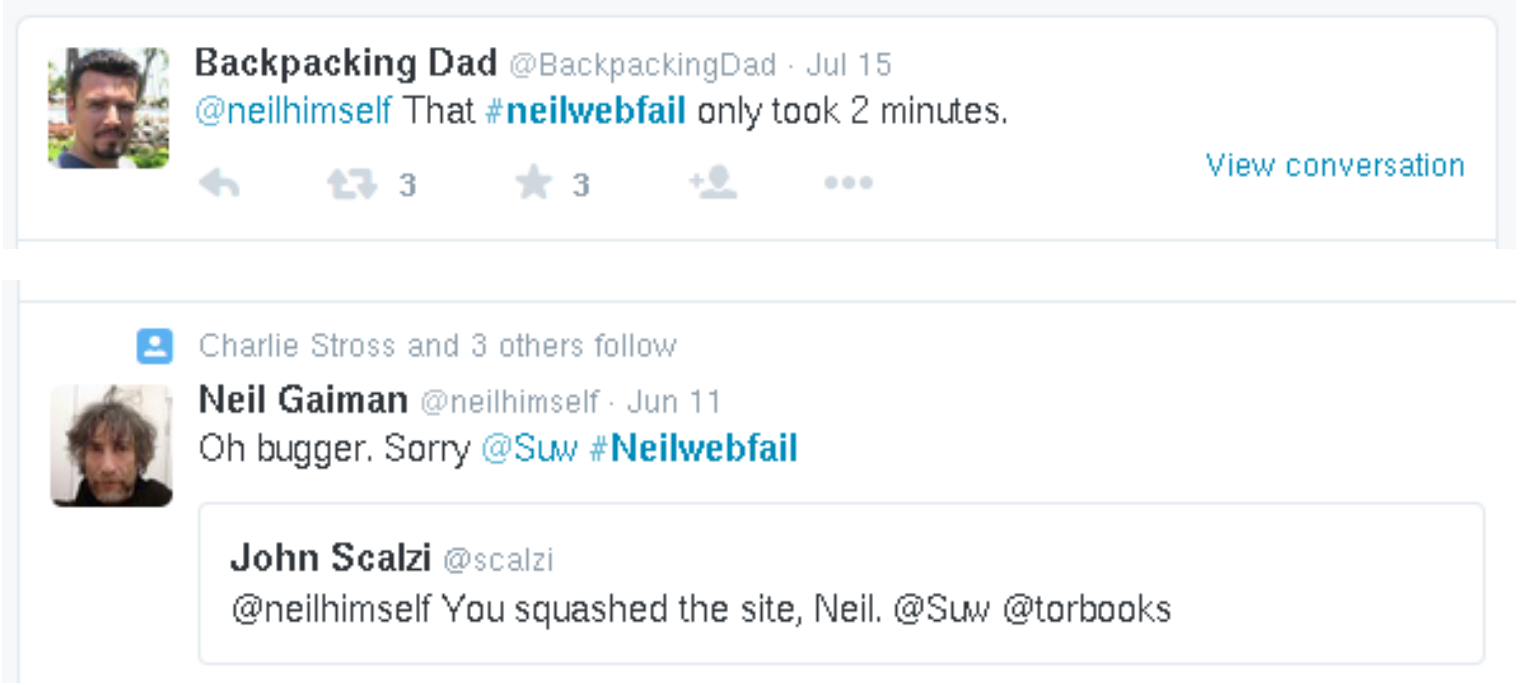
> ”A democracy, if you can keep it”

Do you have the courage to do what Snowden did ?

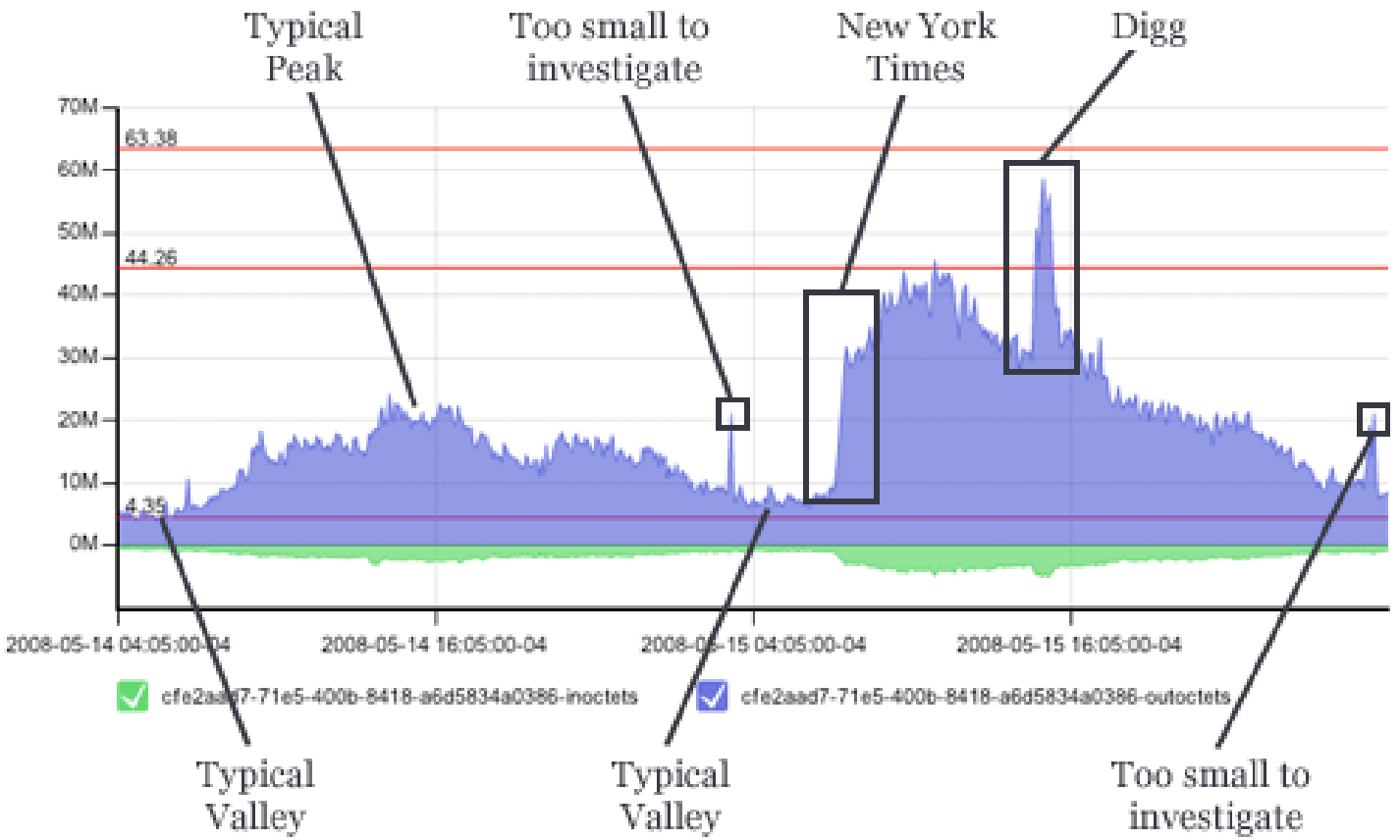
Neil Gaiman

2.3m twitter followers

Twit a link and **boom**!

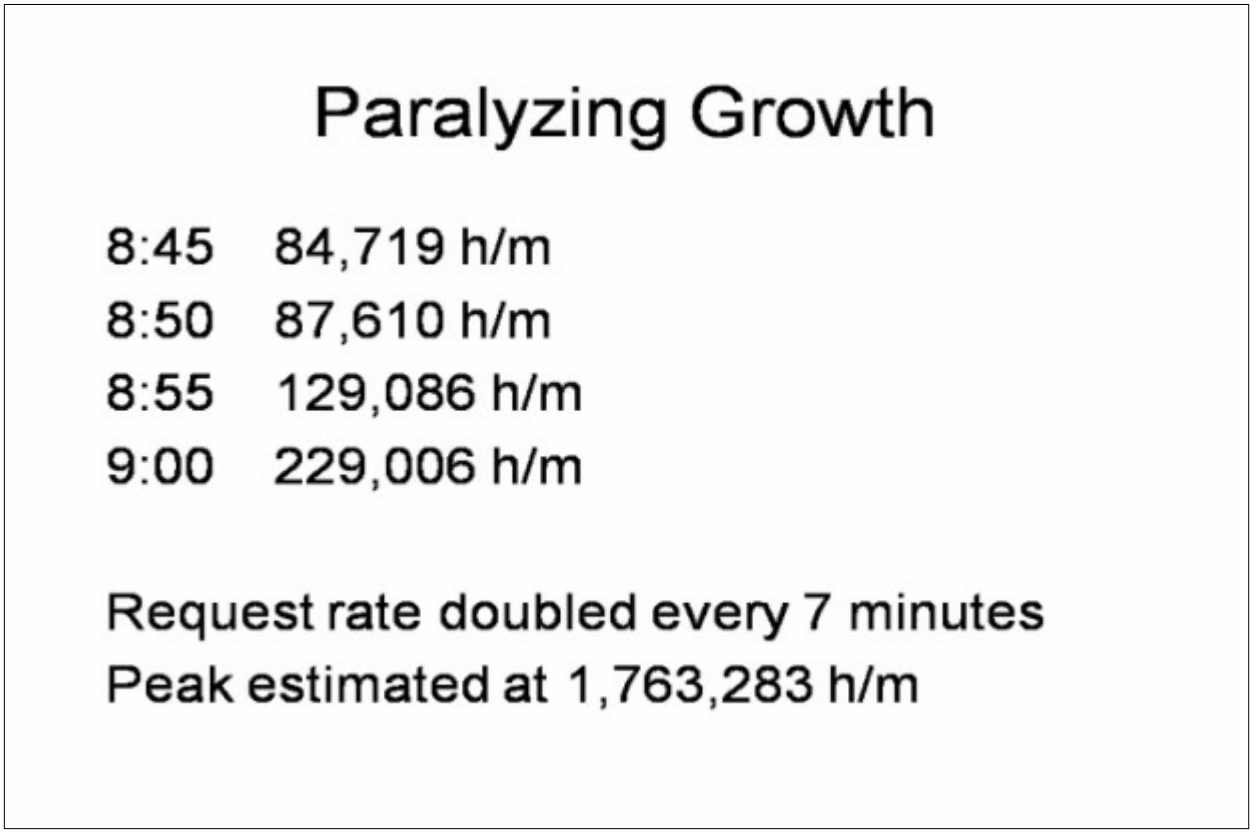


The $BigSiteEffect



Src: Theo Schlossnagle

CNN on 20010911



Willian LeFebvre:
CNN.com Facing a World Crisis
LISA '01

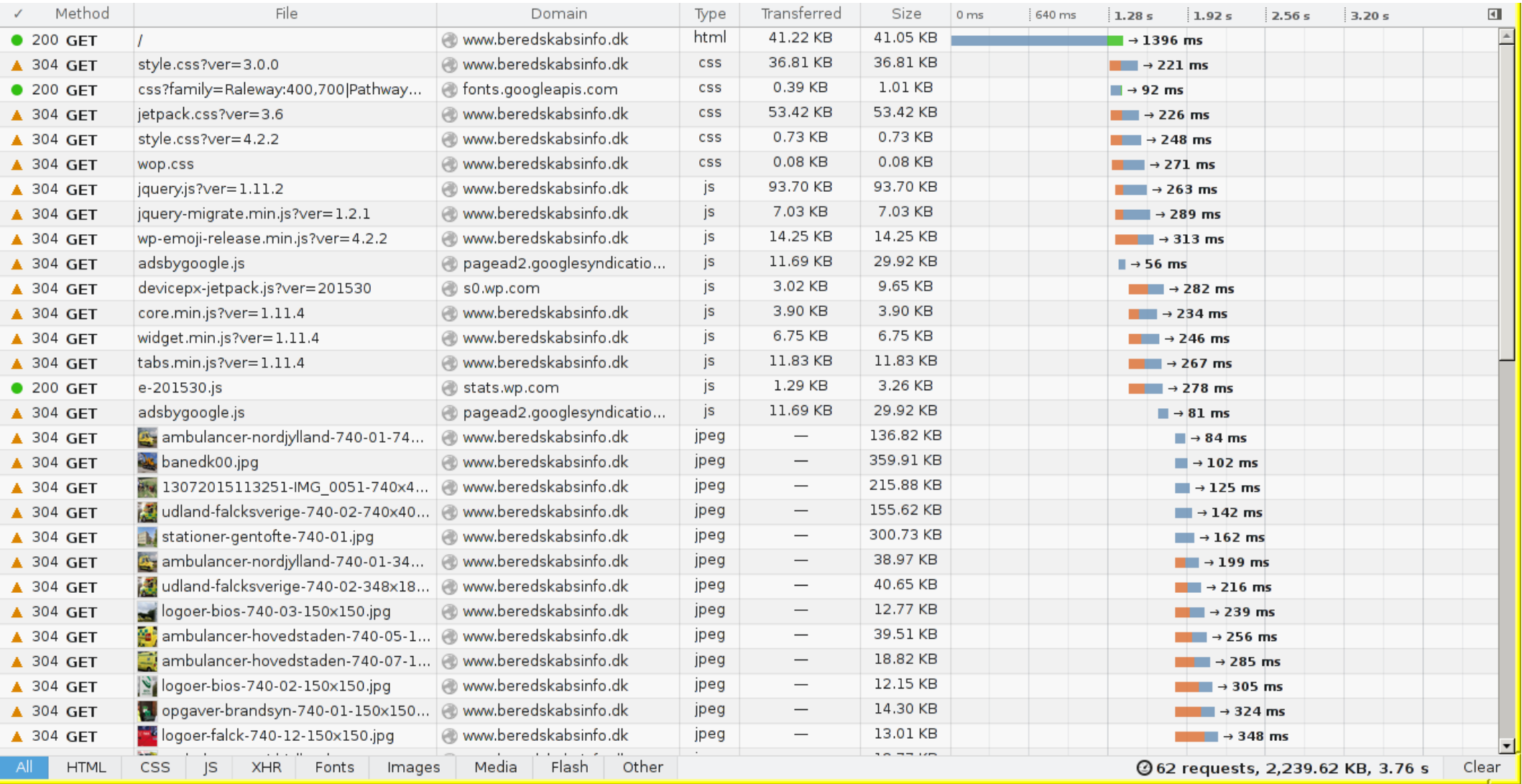
CNN's solution

Scavenge 5 times as many servers

Reduce frontpage to 1247 bytes

I hope they have a (better) plan...

Danish ”FEMA”: 62 req 2.2MB 3.7 sec

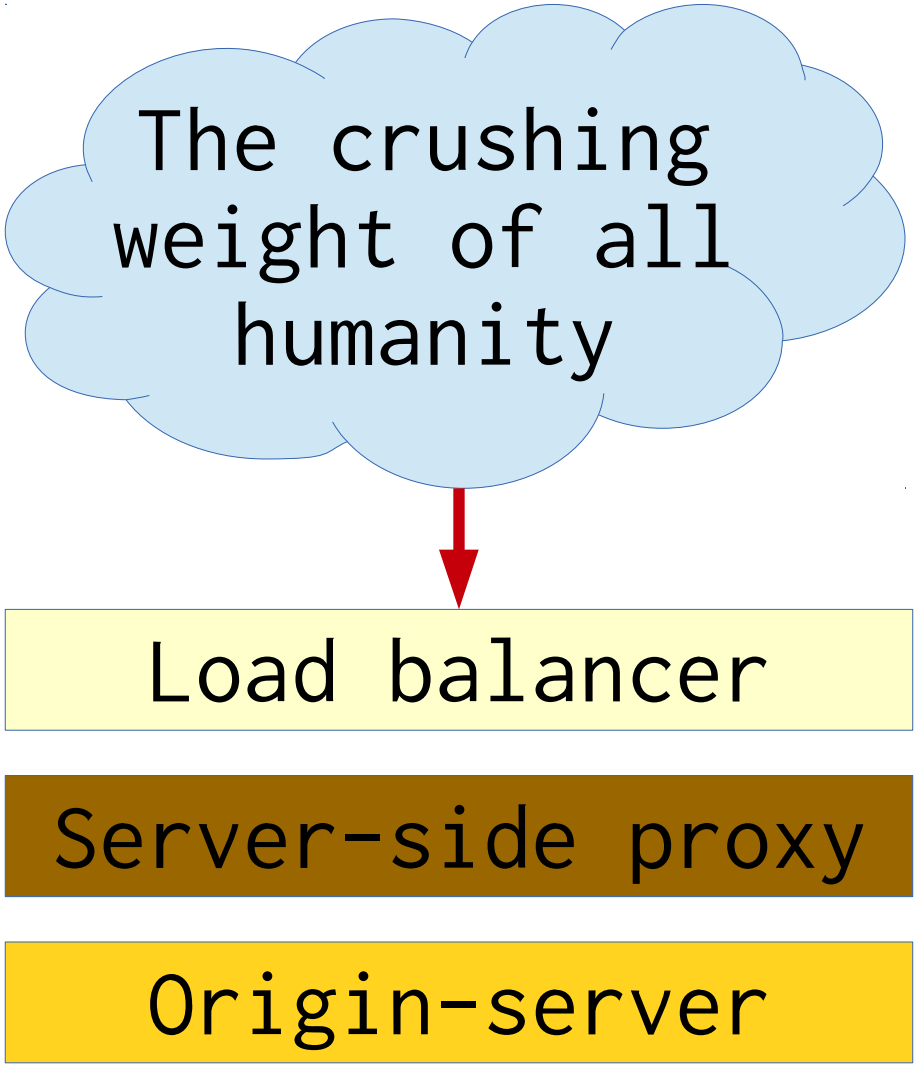


✓	Method	File	Domain	Type	Transferred	Size	0 ms / 640 ms / 1.28 s / 1.92 s / 2.56 s / 3.20 s
●	200 GET	/	www.beredskabsinfo.dk	html	41.22 KB	41.05 KB	→ 1396 ms
▲	304 GET	style.css?ver=3.0.0	www.beredskabsinfo.dk	css	36.81 KB	36.81 KB	→ 221 ms
●	200 GET	css?family=Raleway:400,700|Pathway...	fonts.googleapis.com	css	0.39 KB	1.01 KB	→ 92 ms
▲	304 GET	jetpack.css?ver=3.6	www.beredskabsinfo.dk	css	53.42 KB	53.42 KB	→ 226 ms
▲	304 GET	style.css?ver=4.2.2	www.beredskabsinfo.dk	css	0.73 KB	0.73 KB	→ 248 ms
▲	304 GET	wop.css	www.beredskabsinfo.dk	css	0.08 KB	0.08 KB	→ 271 ms
▲	304 GET	jquery.js?ver=1.11.2	www.beredskabsinfo.dk	js	93.70 KB	93.70 KB	→ 263 ms
▲	304 GET	jquery-migrate.min.js?ver=1.2.1	www.beredskabsinfo.dk	js	7.03 KB	7.03 KB	→ 289 ms
▲	304 GET	wp-emoji-release.min.js?ver=4.2.2	www.beredskabsinfo.dk	js	14.25 KB	14.25 KB	→ 313 ms
▲	304 GET	adsbygoogle.js	pagead2.googlesyndicatio...	js	11.69 KB	29.92 KB	→ 56 ms
▲	304 GET	devicepx-jetpack.js?ver=201530	s0.wp.com	js	3.02 KB	9.65 KB	→ 282 ms
▲	304 GET	core.min.js?ver=1.11.4	www.beredskabsinfo.dk	js	3.90 KB	3.90 KB	→ 234 ms
▲	304 GET	widget.min.js?ver=1.11.4	www.beredskabsinfo.dk	js	6.75 KB	6.75 KB	→ 246 ms
▲	304 GET	tabs.min.js?ver=1.11.4	www.beredskabsinfo.dk	js	11.83 KB	11.83 KB	→ 267 ms
●	200 GET	e-201530.js	stats.wp.com	js	1.29 KB	3.26 KB	→ 278 ms
▲	304 GET	adsbygoogle.js	pagead2.googlesyndicatio...	js	11.69 KB	29.92 KB	→ 81 ms
▲	304 GET	ambulancer-nordjylland-740-01-74...	www.beredskabsinfo.dk	jpeg	—	136.82 KB	→ 84 ms
▲	304 GET	banedk00.jpg	www.beredskabsinfo.dk	jpeg	—	359.91 KB	→ 102 ms
▲	304 GET	13072015113251-IMG_0051-740x4...	www.beredskabsinfo.dk	jpeg	—	215.88 KB	→ 125 ms
▲	304 GET	udland-falcksverige-740-02-740x40...	www.beredskabsinfo.dk	jpeg	—	155.62 KB	→ 142 ms
▲	304 GET	stationer-gentofte-740-01.jpg	www.beredskabsinfo.dk	jpeg	—	300.73 KB	→ 162 ms
▲	304 GET	ambulancer-nordjylland-740-01-34...	www.beredskabsinfo.dk	jpeg	—	38.97 KB	→ 199 ms
▲	304 GET	udland-falcksverige-740-02-348x18...	www.beredskabsinfo.dk	jpeg	—	40.65 KB	→ 216 ms
▲	304 GET	logoer-bios-740-03-150x150.jpg	www.beredskabsinfo.dk	jpeg	—	12.77 KB	→ 239 ms
▲	304 GET	ambulancer-hovedstaden-740-05-1...	www.beredskabsinfo.dk	jpeg	—	39.51 KB	→ 256 ms
▲	304 GET	ambulancer-hovedstaden-740-07-1...	www.beredskabsinfo.dk	jpeg	—	18.82 KB	→ 285 ms
▲	304 GET	logoer-bios-740-02-150x150.jpg	www.beredskabsinfo.dk	jpeg	—	12.15 KB	→ 305 ms
▲	304 GET	opgaver-brandsyn-740-01-150x150...	www.beredskabsinfo.dk	jpeg	—	14.30 KB	→ 324 ms
▲	304 GET	logoer-falck-740-12-150x150.jpg	www.beredskabsinfo.dk	jpeg	—	13.01 KB	→ 348 ms

All | HTML | CSS | JS | XHR | Fonts | Images | Media | Flash | Other

62 requests, 2,239.62 KB, 3.76 s | Clear

Where performance gets sticky



A load balancer is a HTTP-router.

Need just one thing:

Quick way to determine where to route traffic

The more it has to chew the lower the performance

How to route fast

IP-method:

- Fixed size&width adress field
- Route every PDU

The Telephone-method:

- PDU#1: expensive route decision, assign id
- PDU#2-N: ”IP route” on id

HTTP routable fields (typical)

URL, Host, Cookie, Auth

HTTP1:

- URL @ fixed location
- Rest findable with trivial string search
- No memory needed except RX-buffer
- Almost, but not quite, ”IP mode routing”
- Detecting end of PDU is tricky.

HTTP2:

- URL near the front
- All req's decompression, state & memory-alloc
- Telephone-mode per stream

A bit of history...

SAN FRANCISCO — July 28, 1998

Walnut Creek CDROM set the record of transferring 417 gigabytes of files in one day, surpassing Microsoft Corporation's record of transferring approximately 350 gigabytes of files per day during the Windows95 release. Microsoft used more than 40 server machines to achieve the previous record, while Walnut Creek CDROM used a single 200MHz Intel Pentium Pro processor running FreeBSD.

(417 GB/d = T3, machine could do 100Mbit/s)

HTTP/2 at wirespeed ?

That would be 10/40 Gbit/s today

Google havn't heard about it yet

… And probably never will. (hint: 100 Gbit/s)

Possible in hardware? ”Not obvious”

… And that's without SSL

HTTP/2 as a bottleneck

CNN and Civil Defense should stay H1:

- Minimal H1 webpage: 9 pkt, 2 RTT
  - SYN|syn|ACK,DATA,FIN|ack,data,fin|ACK
- Can be delivered in <10 syscalls, <10µs

Scaling H2 up is **much** more expensive than H1

- Small guys & startups fail on success
- = Internet refeudalisation

HTTP/2, the proxy view

Advantages:

- Fewer TCP connections

Disadvantages:

- Much more complex
- Major DoS exposure
- Much more RAM + CPU needed
- Sinks before wire-speed is reached
- ”SSL-everywhere” forces CA-trojan/bogo-cert

Varnish Cache — http://varnish-cache.org

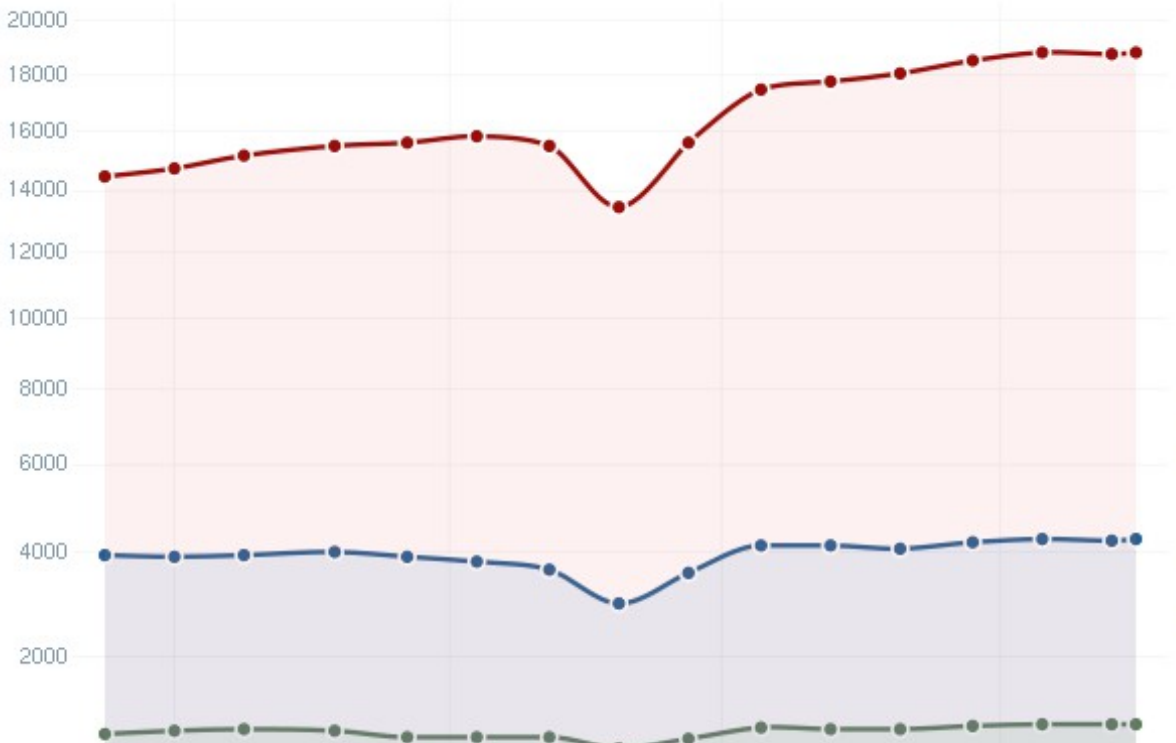
BSD license
84.7 KLOC
90% test coverage
0 Coverity defects

Server-side caching proxy
DSL configuration (”VCL”)
Very fast & scalable
Extensible functionality

Varnish Usage Statistics

Websites using Varnish

Download Lead List



Switch Chart Data

All Top Site Data

Top 10k Sites

Top 100k Sites

Top Million Sites

The Entire Internet

Coverage Totals

Quantcast Top 10k 998 of 10,000	10%
Quantcast Top 100k 4,286 of 100,000	4.3%
Quantcast Top Million 18,816 of 872,343	2.2%
BuiltWith Top Sites	2.4%