HTTP/3 or bust

Poul-Henning Kamp

phk@FreeBSD.org

phk@Varnish.org

@bsdphk

```
$ history

1985-      RISKS, a gentlemens discussion club
2010-06-17 EFF launches ”HTTPS Everywhere”
2012-      FBI snoops on CIA director Petraeus
2013-06-05 First Snowden story in papers (”PRISM”)
2013-06-14 ”STA” ”RT” becomes ”PRI” ”SM”
2014-04-07 HeartBleed ”bug”
2015-03-03 FREAK attack
2015-05    HTTP/2 published
2015-07-10 Apple SSL GotoFail ”bug”
2015-08    RFC7624 Pervasive Surv. is attack
2015-09-24 Bluecoat gets wildcard MiTM cert
2015-12    KZ: Asks Mozilla to include MITM cert
2016-04-12 Let’s Encrypt launched
2016-04    US: Proposed law: mandatory backdoors
2016-06    UK: Proposed law: ”Snoopers Charter”
2016-06-20 RU: Proposed law: msg’er backdoors
```

```
$ history -v

____-__-__ NSAs illegal collection stopped
____-__-__ NSAs illegally collected data destroyed
____-__-__ Scope of NSAs collection published
____-__-__ Punishment of NSA authority exceeded
____-__-__ Law: Clearly limit NSAs authority
____-__-__ Const’nl Amendment: Electronic privacy
____-__-__ Supreme Court rules NSA vs 4th amendment
____-__-__ Law: Defense Counsel access to collection
____-__-__ Treaty: Privacy in the Net and Cloud
____-__-__ Public uprising against snooping
____-__-__ Snooping major theme in elections
____-__-__ Government rolls back state snooping
____-__-__ Privacy improves overall
```

Ads, Ads, Ads, Spam, Ads and Marketing

A visit to a typical ”well monetized” respectable website gives 40-200 servers a bite at your privacy

Real time bidding process (”tag managers”)

Big business, big revenues

Practically no regulation (is respected)

Very popular with intelligence agencies

Your privacy is ”protected” (in transit) by SSL

OK, so we didn't win that one…

State actors goal:

- ✓Defeat secrecy

Our defense ”One-Size-Fits-All”: SSL+CA

What we lost in the politics

SSL+CA does:

- Identification
- Integrity
- Authentication
- Secrecy
- Non-repudiation
- Non-replay

SSL/CA broken/bugged/trojaned → all is lost

Secrecy is the least important crypto

Commerce MUST have:
Authentication + Integrity

Commerce SHOULD have:
Non-replay, Non-repudiation

Commerce MAY have (where allowed by law[1]):
Secrecy

[1] Exchanges (Stocks, currency, derivatives, commodities, metals), Publically Traded companies, Market Power, Beneficial monopolies, COCOM, Wassenaar …

Giving up what we cant win

Secrecy (Gov’t)

PSK may work, modulus SW bugs & laws
Otherwise: Forget it

Governments will legislate legal intercept
… or let spy/police obtain it anyway
(Worst case: Jail suspect until decrypted)

Side Effect:

SSL Certs used for secrecy cannot be trusted for auth, due to spread of MiTM

Accept (minimal) Need to Know

- Secrecy (Powers That Be)
  - Orgs with legal req’d MiTM:
    - Prisons, Stock traders, Police, ATC &c
  - Parental Controls
  - Community Smut Filters, school, library &c

- Detecting existence of comms is usually sufficient
  - Ie:
    - ”Why were you surfing playboy.com ?!”
  - Not:
    - ”How do you rate Miss October ’84 ?”

- Metadata disclosure sufficient in 99.9% of cases

The tough one…

Privacy/Secrecy (Commercial)

Lost cause: JS, Cookies & Money

Reality: Normal people don’t seem to care

My kids generation has never known otherwise:

  <= 18 years old: Google has always existed

See that beach over there ?

Privacy/Secrecy (Commercial)

Client must be 100% in control of info-leaks:

Cookies must die!
Instead: Client controlled session-identifier
Choice between ”persistent” and ”one-time”

UX parameter set must be small
User-Agent must die!
Instead: ”UX: win=1200x800x8,js=7,kbd,pointer”

All traffic must be auditable/blockable by user

JS must be disabled

The things we can agree on

Authentication/Integrity/non-repu/non-replay

No goverment want to ruin this

Per object signature with sig-only certs

Governments love trustworthy sig-only certs

- necessary for eGov
- May even (want to) issue them (already)

HTTP/3 — new semantics

Each transaction has up to four parts:

Plain-text metadata

Protected metadata

Protected data

Protected signature(s)

HTTP/3 outline

Delivery metadata (”the envelope”)

- Info necessary for HTTP traffic engineering
  - Out-of-the-blue: {Method, Host, URL}
  - Then: Session-ID: (a nonce)
  - Proxy-instructions

Sent in the clear:

- Faster for load-balancers & caches
- Reduces need for MiTM to break open the rest

HTTP/3 outline

Protected {metadata + data [+ signature(s)]}

Secrecy encryption:

- Trustworth: Pre-Shared-Keys
- Strong: Secrecy-cert from CA
  - Protects against non-state-level actors
- Weak: Inline key
  - (=scrambling -> public cacheable)
  - Still protects against 'tcpdump|grep'

Protected metadata contains:

- Signature (auth/integrity)
- Content-Type, …

HTTP/3 outline

Signatures

Here,<signature(s)>
Precomputed

Trailing(,hash=sha256,salt=kzdLbXFCpNx)
Streaming

hash up front → Enable one-pass sig-check

Detached
Batched, precomputed

HTTP/3 outline

Detached signatures

```
index.html   sig=detached,/content.auth
style.css    sig=detached,/content.auth
script.js    sig=detached,/content.auth
cust.json    sig=here,clrIVSMXU6xHypJ1mw+I+X12E1U
content.auth sig=trailing,hash=sha256
```

content.auth (can be cacheable):

```
   index.html signature
   style.css signature1,signature2,signature3
   script.js signature
   subpage1.html signature
   subpage2.html signature
   ...
```