Proxies in HTTP

A Chair's View

“Proxies Are **Useful**”

- to **Enforce Policy** in schools & prisons; by parents & workplaces
- to **Optimise** on satellite, bad connections, crowded nets
- to **Enhance** with annotations, virus scanning, ad blocking
- to **Understand** user behaviour, network utilisation, protocol behaviour

“Proxies are **Dangerous**”

- they inhibit **protocol evolution**
- they introduce **errors**
- they aid **authoritarian regimes**
- they’re a threat to **Network Neutrality** (?)
- they turn a **2-body problem** into a **3-body problem**

Pervasive **Encryption** & “**Split** Browsers”

What does the **spec** say?

A “proxy” is a message-forwarding agent that is **selected by the client**, usually via local configuration rules… Proxies are often used to group an organization's HTTP requests through a common intermediary for the sake of security, annotation services, or shared caching. Some proxies are **designed to apply transformations** to selected messages or payloads while they are being forwarded, as described in Section 5.7.2.

– RFC7230, Section 2.3

“Some intermediaries include features for transforming messages and their payloads. A proxy might, for example, convert between image formats in order to save cache space or to **reduce the amount of traffic on a slow link**. However, operational problems might occur when these transformations are applied payloads intended for critical applications.”

- RFC7230, Section 5.7.2

“[For HTTPS URIs,] the user agent MUST ensure that its connection to the origin server is secured through the use of **strong encryption, end-to-end**, prior to sending the first HTTP request.”

–RFC7230, section 2.7.2

“[HTTPS] implies **end-to-end security**.”

–RFC7230, section A.2

Summing Up

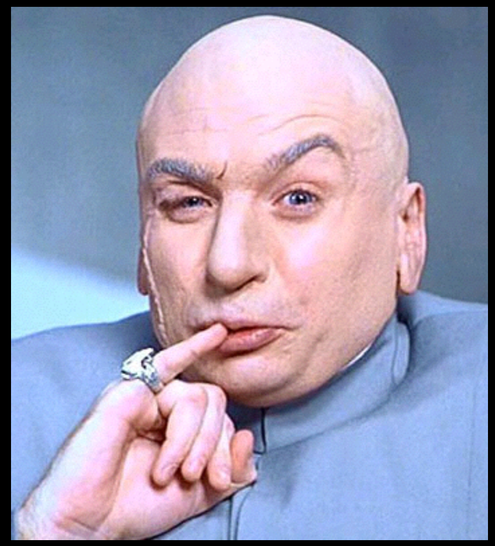
- Proxies can **transform messages** (within limits)
- Proxies are **explicitly configured** by the client
- https:// is **end-to-end**

Changing **any** of these requires overcoming consensus reflected in multiple RFCs and more than two decades of adoption.

This is not a matter of adding some new features; it's changing the nature of an implicit contract between the users of HTTP.

All of them.

…even though *yes, we know that some people break it sometimes*.



The IETF is **bad** at political, economic and legal issues, and **does not take sides** on these matters.

We do seek to enable the
“**Tussle in Cyberspace**”

Clark, Wroclawski, Sollins & Braden, SIGCOMM 2002

…but changing the nature of HTTP unilaterally is **taking sides**, **not** enabling “the tussle”.

“In the Internet age, a whole new sphere of de facto lawmaking has emerged in the guise of software code and technical standards that channel and constrain what people do with their technology.”

Rebecca McKinnon,
Consent of the Networked

"Even the mere possibility of communications information being captured creates an interference with privacy, with a potential chilling effect on rights, including those to free expression and association."

"The right to privacy in the digital age"
Report of the Office of the United Nations
High Commissioner for Human Rights

What **Can** We Do?

- Publish “Proxy Problem” draft
- Standardise Proxy.pac
- Find other ways to address underlying use cases
- …