Network Working Group
Internet-Draft
Intended status: Informational
Expires: April 24, 2014

M. Nottingham
October 21, 2013

The "safe" HTTP Client Hint
draft-nottingham-safe-hint-00

Abstract

This specification defines a "safe" HTTP Client Hint, expressing a user preference to avoid "objectionable" content.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on April 24, 2014.

Table of Contents

1. Introduction

Many Web sites have a "safe" mode, to assist those who don't want to be exposed to "objectionable" content, or who don't want their children to be exposed to such content. YouTube [youtube], Yahoo! Search [yahoo], Google Search [google], Bing Search [bing], and many other services have such a setting.

However, a user that wishes to have this preference honoured would need to go to each Web site in turn, navigate to the appropriate page, (possibly creating an account along the way) to get a cookie [RFC6265] set in the browser. They would need to do this for each browser on every device they use. As has been widely noted, this is difficult [age-privacy].

This can be onerous to nearly impossible to achieve effectively, because there are too many permutations of sites, user agents and devices.

If instead this preference is proactively advertised by the user agent, things become much simpler. A user agent that supports this (whether it be an individual browser, or through an Operating System HTTP library) need only be configured once to assure that the preference is advertised to all sites that understand and choose to act upon it. It's no longer necessary to go to each site that has potentially "unsafe" content and configure a "safe" mode.

Furthermore, a proxy (for example, at a school) can be used to ensure that the preference is associated with all (unencrypted) requests flowing through it, helping to assure that clients behind it are not exposed to "objectionable" content.

This specification defines how to associate this preference with a request, as a HTTP Client Hint [grigorik-http-client-hints].

Note that this approach does not define what "safe" is; rather, it is interpreted within the scope of each Web site that chooses to act upon this information (or not). As such, it does not require agreement upon what "safe" is, nor does it require application of policy in the user agent or an intermediary (which can be problematic for many reasons).

1.1. Notational Conventions

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119].

2. The "safe" HTTP Client Hint

When present in a request, the "safe" HTTP Client Hint indicates that the user prefers content which is not objectionable, according to the server's definition of the concept.

For example a request that includes the "safe" hint:

```
GET /foo.html HTTP/1.1
Host: www.example.org
User-Agent: ExampleBrowser/1.0
CH: safe
```

When configured to do so, user agents SHOULD include the "safe" hint in every request, to ensure that the preference is applied (where possible) to all resources.

For example, a Web browser might have a "Request Safe Browsing" preference option. additionally, other clients MAY insert it; e.g., an operating system might choose to insert the hint in requests based upon system-wide preferences, or a proxy might do so based upon its configuration.

Servers that utilise the "safe" hint SHOULD document that they do so, along with the criteria that they use to denote objectionable content. If a site has more fine-grained degrees of "safety", it SHOULD select a reasonable default to use, and document that; it MAY use additional mechanisms (e.g., cookies) to fine-tune.

A response corresponding to the request above might have headers that look like this:

```
HTTP/1.1 200 OK
Transfer-Encoding: chunked
Content-Type: text/html
Server: ExampleServer/2.0
Vary: CH
```

Note that the Vary response header needs to be sent if responses associated with the resource might change depending on the value of the "CH" header; this is not only true for those responses that have changed, but also the "default" unchanged responses.

3. Security Considerations

The "safe" client hint is not a secure mechanism; it can be inserted or removed by intermediaries with access to the data stream. Its presence reveals information about the user, which may be of small

assistance in "fingerprinting" the user (1 bit of information, to be precise).

Due to its nature, including it in requests does not assure that all content will actually be safe; it is only when servers elect to honour it that it might change content.

Even then, a malicious server might adapt content so that it is even less "safe" (by some definition of the word). As such, this mechanism on its own is not enough to assure that only "safe" content is seen; users who wish to ensure that will need to combine its use with other techniques (e.g., content filtering).

Furthermore, the server and user may have differing ideas regarding the semantics of "safe." As such, the "safety" of the user's experience when browsing from site to site might (and probably will) change.

4. IANA Considerations

This specification registers the "safe" HTTP Client Hint [grigorik-http-client-hints]:

- Hint Name: safe
- Hint Value: boolean
- Description: Indicates that the user (or one responsible for them) prefers "safe" / "unobjectionable" content.
- Contact: mnot@mnot.net
- Specification: (this document)
- Notes:

5. References

5.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[grigorik-http-client-hints] Grigorik, I., "HTTP Client Hints", 2013.

5.2. Informative References

[RFC6265] Barth, A., "HTTP State Management Mechanism", RFC 6265, April 2011.

[age-privacy] Moses, A., "Privacy concern as apps share data from kids left to their own devices", 2012, <http://www.theage.com.au/technology/technology-news/privacy-concern-as-apps-share-data-from-kids-left-to-their-own-devices-20121222-2bso6.html>.

[bing] Microsoft, "Bing Help: Block Explicit Web Sites", 2013, <http://onlinehelp.microsoft.com/en-AU/bing/ff808441.aspx>.

[google] Google, "SafeSearch: turn on or off", 2013, <http://support.google.com/websearch/bin/answer.py?p=settings_safesearch&answer=510>.

[yahoo] Yahoo! Inc., "Yahoo! Search Preferences", 2013, <http://search.yahoo.com/preferences/preferences>.

[youtube] Google, "How to access and turn on Safety Mode?", 2013, <http://support.google.com/youtube/bin/answer.py?answer=174084>.

Appendix A. Acknowledgements

Thanks to Alissa Cooper, Ilya Grigorik and Emma Llanso for their comments.

Author's Address

Mark Nottingham

EMail: mnot@mnot.net
URI: http://www.mnot.net/