httpstate	A. Barth
Internet-Draft	Google, Inc.
Intended status: Standards Track	March 06, 2011
Expires: September 07, 2011	

Origin Cookies
draft-abarth-cake-01

Abstract

This document defines the Origin attribute for cookies, which lets servers harmonize the security policy of their cookies with the widely used same-origin policy. Origin cookies provide both confidentiality and integrity, unlike the Secure attribute, which provides only confidentiality.

Editorial Note (To be removed by RFC Editor)

If you have suggestions for improving this document, please send email to mailto:http-state@ietf.org. Further Working Group information is available from https://tools.ietf.org/wg/httpstate/.

Status of this Memo

Copyright Notice

Table of Contents

1. Introduction

TODO
This document defines the Origin attribute for cookies, which lets servers harmonize the security policy of their cookies with the widely used same-origin policy. Origin cookies provide both confidentiality and integrity, unlike the Secure attribute, which provides only confidentiality.

2. Conventions

2.1. Conformance Criteria

The key words "MUST", "MUST NOT", "REQUIRED", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119].
Requirements phrased in the imperative as part of algorithms (such as "strip any leading space characters" or "return false and abort these steps") are to be interpreted with the meaning of the key word ("MUST", "SHOULD", "MAY", etc) used in introducing the algorithm.
Conformance requirements phrased as algorithms or specific steps can be implemented in any manner, so long as the end result is equivalent. In particular, the algorithms defined in this specification are intended to be easy to understand and are not intended to be performant.

2.2. Syntax Notation

This specification uses the Augmented Backus-Naur Form (ABNF) notation of [RFC5234].

The following core rules are included by reference, as defined in [RFC5234], Appendix B.1: ALPHA (letters), CR (carriage return), CRLF (CR LF), CTL (controls), DIGIT (decimal 0-9), DQUOTE (double quote), HEXDIG (hexadecimal 0-9/A-F/a-f), LF (line feed), OCTET (any 8-bit sequence of data), SP (space), HTAB (horizontal tab), CHAR (any US-ASCII character), VCHAR (any visible US-ASCII character), and WSP (whitespace).

2.3. Terminology

The terms user agent, client, server, proxy, origin server, request-host, and request-uri have the same meaning as in cookie specification ([cite: Cookies], Section 2.3).
Two sequences of octets are said to case-insensitively match each other if and only if they are equivalent under the i;ascii-casemap collation defined in [RFC4790].
The term string means a sequence of octets.

3. Overview

Using the Origin attribute, a server can set a cookie for its origin. Unlike the Path, Domain, and Secure attributes, the Origin attribute harmonizes the security properties of the cookie with the same-origin policy [cite: Principles of Origin]. In particular, the Origin attribute provides both confidentiality and integrity from other origins.
The Origin attribute superceeds the Path, Domain, and Secure attributes. The server can set these attributes as well to control the scope of cookies in legacy user agents. User agents that support origin cookies will ignore these attributes when the Origin attribute is present.
Origin cookies are returned from the user agent to the server in the Origin-Cookie header field and not the Cookie header field because the Cookie header field does not provide any information about the source of the cookie. When the server receives a cookie in the Origin-Cookie header field, the server can reason that the cookie was set by its own origin, and not injected by another origin.

3.1. Examples

The server can set an origin cookie, which is returned in the Origin-Cookie header field. Origin cookies support all the same attributes as other kinds of cookies, except Path, Domain, and Secure, which are ignored.
== Server -> User Agent ==

Set-Cookie: SID=31d4d96e407aad42; Origin

== User Agent -> Server ==

Origin-Cookie: SID=31d4d96e407aad42

Non-origin cookies are returned in the Cookie header as usual. If the user agent sends the server both origin and non-origin cookies, the origin cookies are returned in the Origin-Cookie header field and the non-origin cookies are returned in the Origin-Cookie header field.

```
== Server -> User Agent ==

Set-Cookie: SID=31d4d96e407aad42; Origin
Set-Cookie: lang=en-US; Path=/; Domain=example.com


== User Agent -> Server ==

Cookie: lang=en-US
Origin-Cookie: SID=31d4d96e407aad42
```

4. Server Requirements

TODO

5. User Agent Requirements

TODO

6. Privacy Considerations

TODO

7. Security Considerations

TODO

8. IANA Considerations

The permanent message header registry (see [RFC3864]) should be updated with the following registrations:

8.1. Origin-Cookie

Header field name: Origin-Cookie
Applicable protocol: http
Status: standard
Author/Change controller: IETF
Specification document: this specification

9. References

9.1. Normative References

[RFC2119]	Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels ", BCP 14, RFC 2119, March 1997.
[RFC2616]	Fielding, R., Gettys, J., Mogul, J., Frystyk, H., Masinter, L., Leach, P. and T. Berners-Lee, "Hypertext Transfer Protocol -- HTTP/1.1", RFC 2616, June 1999.
[RFC4790]	Newman, C., Duerst, M. and A. Gulbrandsen, "Internet Application Protocol Collation Registry", RFC 4790, March 2007.
[RFC5234]	Crocker, D. and P. Overell, "Augmented BNF for Syntax Specifications: ABNF ", STD 68, RFC 5234, January 2008.

9.2. Informative References

[RFC3864]	Klyne, G., Nottingham, M. and J. Mogul, "Registration Procedures for Message Header Fields", BCP 90, RFC 3864, September 2004.

Appendix A. Acknowledgements

TODO

Author's Address

Adam Barth Barth Google, Inc. EMail: ietf@adambarth.com URI: http://www.adambarth.com/