

Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: November 27, 2016

M. Thomson
C. Peterson
Mozilla
May 26, 2016

Expiring Aggressively Those HTTP Cookies
draft-thomson-http-omnomnom-00

Abstract

HTTP Cookies that are sent over connections without confidentiality and integrity protection are vulnerable to theft. Such cookies should be expired aggressively.

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 November 27, 2016.

Copyright Notice

Copyright (c) 2016 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to [BCP 78](#) and the IETF Trust's Legal Provisions Relating to IETF Documents (<http://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

- [1.](#) Introduction [2](#)
- [1.1.](#) Notational Conventions [2](#)
- [2.](#) Expire Cookies [2](#)
- [3.](#) Security Considerations [3](#)
- [4.](#) IANA Considerations [3](#)
- [5.](#) References [3](#)
- [5.1.](#) Normative References [3](#)
- [5.2.](#) Informative References [4](#)
- [Appendix A.](#) Acknowledgements [4](#)
- Authors' Addresses [4](#)

1. Introduction

HTTP cookies [[RFC6265](#)] provide a means of persisting server state between multiple requests. This feature is widely used on both HTTP [[RFC7230](#)] and HTTPS [[RFC2818](#)] requests.

The authority for "http://" resources (see [Section 9.1 of \[RFC7230\]](#)) derives from insecure sources: notably the network and the DNS (absent DNSSEC). This situation might change over time. As persistent state, cookies create a way for an attacker to link requests. The information that a cookie holds might also be valuable to that attacker in some way.

To limit the effectiveness of attacks on cleartext communications [[RFC7258](#)], user agents are encouraged to limit the persistence of cookies that are set over insecure connections.

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. Expire Cookies

Cookies that are set using insecure channels (i.e., HTTP over cleartext TCP), MUST have a short time limit on the time that they are persisted. For instance, such cookies might only persist until the user closes their browser.

If a user agent detects a change in network conditions it SHOULD remove any cookies that were established using insecure channels.

Alternatives:

- o In the investigation into this change, it was suggested that cookies without the "Secure" flag might be given the same treatment. However, this resulted in a far greater number of cookies being affected and some interoperability problems as a result.
- o This change might be limited to cookies that are set in third-party contexts. See [I-D.west-first-party-cookies].

Limiting access to third-party cookies in this fashion could have the secondary effect of encouraging providers of third-party content to move to HTTPS. This removes that content as a barrier to the adoption of HTTPS for the sites that include that content.

3. Security Considerations

This document describes an improvement that could be a security improvement. However, this is not without risks. For cookies that are used as a substitute for logins, more regular clearing of a login cookie could expose the primary authentication token (for instance, a password) to more network attackers as a result of being entered more often.

Clearing login tokens could also cause a degree of user annoyance, as login information is lost. Such annoyance manifests in many subtle ways.

Limiting the change to third-party contexts as suggested above might reduce these risks, though with lesser overall impact.

4. IANA Considerations

This document makes no request of IANA.

5. References

5.1. Normative References

- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", [BCP 14](#), [RFC 2119](#), DOI 10.17487/RFC2119, March 1997, <<http://www.rfc-editor.org/info/rfc2119>>.
- [RFC6265] Barth, A., "HTTP State Management Mechanism", [RFC 6265](#), DOI 10.17487/RFC6265, April 2011, <<http://www.rfc-editor.org/info/rfc6265>>.

[RFC7230] Fielding, R., Ed. and J. Reschke, Ed., "Hypertext Transfer Protocol (HTTP/1.1): Message Syntax and Routing", [RFC 7230](#), DOI 10.17487/RFC7230, June 2014, <<http://www.rfc-editor.org/info/rfc7230>>.

5.2. Informative References

[RFC2818] Rescorla, E., "HTTP Over TLS", [RFC 2818](#), DOI 10.17487/RFC2818, May 2000, <<http://www.rfc-editor.org/info/rfc2818>>.

[RFC7258] Farrell, S. and H. Tschofenig, "Pervasive Monitoring Is an Attack", [BCP 188](#), [RFC 7258](#), DOI 10.17487/RFC7258, May 2014, <<http://www.rfc-editor.org/info/rfc7258>>.

Appendix A. Acknowledgements

Henri Sivonen first suggested that non-Secure cookies be made ephemeral. Chris Peterson did much of the initial investigation and work. See <https://bugzilla.mozilla.org/show_bug.cgi?id=1160368> for details.

Authors' Addresses

Martin Thomson
Mozilla

Email: martin.thomson@gmail.com

Chris Peterson
Mozilla

Email: cpeterson@mozilla.com

