

httpstate	A. Barth	
Internet-Draft	U.C. Berkeley	
Obsoletes: 2109 (if approved)	October 10, 2010	
Intended status: Standards Track		
Expires: April 13, 2011		

[TOC](#)

HTTP State Management Mechanism draft-ietf-httpstate-cookie-15

Abstract

This document defines the HTTP Cookie and Set-Cookie header fields. These header fields can be used by HTTP servers to store state (called cookies) at HTTP user agents, letting the servers maintain a stateful session over the mostly stateless HTTP protocol. Although cookies have many historical infelicities that degrade their security and privacy, the Cookie and Set-Cookie header fields are widely used on the Internet.

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>. Suggestions with test cases are especially appreciated. Further Working Group information is available from <https://tools.ietf.org/wg/httpstate/>.

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 13, 2011.

Copyright Notice

Copyright (c) 2010 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.

This document may contain material from IETF Documents or IETF Contributions published or made publicly available before November 10, 2008. The person(s) controlling the copyright in some of this material may not have granted the IETF Trust the right to allow modifications of such material outside the IETF Standards Process. Without obtaining an adequate license from the person(s) controlling the copyright in such materials, this document may not be modified outside the IETF Standards Process, and derivative works of it may not be created outside the IETF Standards Process, except to format it for publication as an RFC or to translate it into languages other than English.

Table of Contents

- [1.](#) Introduction
- [2.](#) Conventions
 - [2.1.](#) Conformance Criteria
 - [2.2.](#) Syntax Notation
 - [2.3.](#) Terminology
- [3.](#) Overview
 - [3.1.](#) Examples
- [4.](#) Server Requirements
 - [4.1.](#) Set-Cookie
 - [4.1.1.](#) Syntax
 - [4.1.2.](#) Semantics (Non-Normative)
 - [4.2.](#) Cookie
 - [4.2.1.](#) Syntax
 - [4.2.2.](#) Semantics
- [5.](#) User Agent Requirements
 - [5.1.](#) Subcomponent Algorithms
 - [5.1.1.](#) Dates
 - [5.1.2.](#) Canonicalized host names
 - [5.1.3.](#) Domain matching
 - [5.1.4.](#) Paths and path-match
 - [5.2.](#) The Set-Cookie Header
 - [5.2.1.](#) The Expires Attribute

5.2.2.	The Max-Age Attribute
5.2.3.	The Domain Attribute
5.2.4.	The Path Attribute
5.2.5.	The Secure Attribute
5.2.6.	The HttpOnly Attribute
5.3.	Storage Model
5.4.	The Cookie Header
6.	Implementation Considerations
6.1.	Limits
6.2.	Application Programming Interfaces
6.3.	IDNA dependency and migration
7.	Privacy Considerations
7.1.	Third-Party Cookies
7.2.	User Controls
8.	Security Considerations
8.1.	Overview
8.2.	Ambient Authority
8.3.	Clear Text
8.4.	Session Identifiers
8.5.	Weak Confidentiality
8.6.	Weak Integrity
8.7.	Reliance on DNS
9.	IANA Considerations
9.1.	Cookie
9.2.	Set-Cookie
10.	References
10.1.	Normative References
10.2.	Informative References
Appendix A.	Acknowledgements
S	Author's Address

1. Introduction

[TOC](#)

This document defines the HTTP Cookie and Set-Cookie header fields. Using the Set-Cookie header field, an HTTP server can pass name/value pairs and associated metadata (called cookies) to a user agent. When the user agent makes subsequent requests to the server, the user agent uses the metadata and other information to determine whether to return the name/value pairs in the Cookie header.

Although simple on its surface, cookies have a number of complexities. For example, the server indicates a scope for each cookie when sending them to the user agent. The scope indicates the maximum amount of time the user agent should return the cookie, the servers to which the user agent should return the cookie, and the URI schemes for which the cookie is applicable.

For historical reasons, cookies contain a number of security and privacy infelicities. For example, a server can indicate that a given cookie is intended for "secure" connections, but the Secure attribute does not provide integrity in the presence of an active network attackers. Similarly, cookies for a given host are shared across all the ports on that host, even though the usual "same-origin policy" used by web browsers isolates content retrieved via different ports. Prior to this document, there were at least three descriptions of cookies: the so-called "Netscape cookie specification" [\[Netscape\] \(Netscape Communications Corp., "Persistent Client State -- HTTP Cookies," 1999.\)](#), RFC 2109 [\[RFC2109\] \(Kristol, D. and L. Montulli, "HTTP State Management Mechanism," February 1997.\)](#), and RFC 2965 [\[RFC2965\] \(Kristol, D. and L. Montulli, "HTTP State Management Mechanism," October 2000.\)](#). However, none of these documents describe how the Cookie and Set-Cookie headers are actually used on the Internet (see [\[Kri2001\] \(Kristol, D., "HTTP Cookies: Standards, Privacy, and Politics," November 2001.\)](#) for historical context). This document attempts to specify the syntax and semantics of these headers as they are actually used on the Internet.

2. Conventions

[TOC](#)

2.1. Conformance Criteria

[TOC](#)

The keywords "MUST", "MUST NOT", "REQUIRED", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [\[RFC2119\] \(Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels," March 1997.\)](#).

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.

[TOC](#)

2.2. Syntax Notation

This specification uses the Augmented Backus-Naur Form (ABNF) notation of [\[RFC5234\] \(Crocker, D., Ed. and P. Overell, "Augmented BNF for Syntax Specifications: ABNF," January 2008.\)](#).

The following core rules are included by reference, as defined in [\[RFC5234\] \(Crocker, D., Ed. and P. Overell, "Augmented BNF for Syntax Specifications: ABNF," January 2008.\)](#), 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).

The OWS (optional whitespace) rule is used where zero or more linear whitespace characters MAY appear:

```
OWS           = *( [ obs-fold ] WSP )
               ; "optional" whitespace
obs-fold      = CRLF
```

OWS SHOULD either not be produced or be produced as a single SP character.

2.3. Terminology

[TOC](#)

The terms user agent, client, server, proxy, and origin server have the same meaning as in the HTTP/1.1 specification ([\[RFC2616\] \(Fielding, R., Gettys, J., Mogul, J., Frystyk, H., Masinter, L., Leach, P., and T. Berners-Lee, "Hypertext Transfer Protocol -- HTTP/1.1," June 1999.\)](#), Section 1.3).

The request-host is the name of the host, as known by the user agent, to which the user agent is sending an HTTP request or is receiving an HTTP response from (i.e., the name of the host to which it sent the corresponding HTTP request).

The term request-uri is defined in Section 5.1.2 of [\[RFC2616\] \(Fielding, R., Gettys, J., Mogul, J., Frystyk, H., Masinter, L., Leach, P., and T. Berners-Lee, "Hypertext Transfer Protocol -- HTTP/1.1," June 1999.\)](#).

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 [\[RFC4790\] \(Newman, C., Duerst, M., and A. Gulbrandsen, "Internet Application Protocol Collation Registry," March 2007.\)](#).

The term string means a sequence of octets.

[TOC](#)

3. Overview

This section outlines a way for an origin server to send state information to a user agent and for the user agent to return the state information to the origin server.

To store state, the origin server includes a Set-Cookie header in an HTTP response. In subsequent requests, the user agent returns a Cookie request header to the origin server. The Cookie header contains cookies the user agent received in previous Set-Cookie headers. The origin server is free to ignore the Cookie header or use its contents for an application-defined purpose.

Origin servers can send a Set-Cookie response header with any response. An origin server can include multiple Set-Cookie header fields in a single response.

Note that folding multiple Set-Cookie header fields into a single header field might change the semantics of the header because the %x2C (",") character is used by the Set-Cookie header in a way that conflicts with such folding. This historical infelicity is incompatible with the usual mechanism for folding HTTP headers as defined in [\[RFC2616\] \(Fielding, R., Gettys, J., Mogul, J., Frystyk, H., Masinter, L., Leach, P., and T. Berners-Lee, "Hypertext Transfer Protocol -- HTTP/1.1," June 1999.\)](#).

3.1. Examples

[TOC](#)

Using the Set-Cookie header, a server can send the user agent a short string in an HTTP response that the user agent will return in future HTTP requests. For example, the server can send the user agent a "session identifier" named SID with the value 31d4d96e407aad42. The user agent then returns the session identifier in subsequent requests.

== Server -> User Agent ==

Set-Cookie: SID=31d4d96e407aad42

== User Agent -> Server ==

Cookie: SID=31d4d96e407aad42

The server can alter the default scope of the cookie using the Path and Domain attributes. For example, the server can instruct the user agent to return the cookie to every path and every subdomain of example.com.

== Server -> User Agent ==

Set-Cookie: SID=31d4d96e407aad42; Path=/; Domain=example.com

== User Agent -> Server ==

Cookie: SID=31d4d96e407aad42

As shown in the next example, the server can store multiple cookies at the user agent. For example, the server can store a session identifier as well as the user's preferred language by returning two Set-Cookie header fields. Notice that the server uses the Secure and HttpOnly attributes to provide additional security protections for the more-sensitive session identifier (see [Section 4.1.2 \(Semantics \(Non-Normative\)\)](#).)

== Server -> User Agent ==

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

== User Agent -> Server ==

Cookie: SID=31d4d96e407aad42; lang=en-US

Notice that the Cookie header above contains two cookies, one named SID and one named lang. If the server wishes the user agent to persist the cookie over multiple "sessions" (e.g., user agent restarts), the server can specify an expiration date in the Expires attribute. Note that the user agent might delete the cookie before the expiration date if the user agent's cookie store exceeds its quota or if the user manually deletes the server's cookie.

== Server -> User Agent ==

Set-Cookie: lang=en-US; Expires=Wed, 09 Jun 2021 10:18:14 GMT

== User Agent -> Server ==

Cookie: SID=31d4d96e407aad42; lang=en-US

Finally, to remove a cookie, the server returns a Set-Cookie header with an expiration date in the past. The server will be successful in removing the cookie only if the Path and the Domain attribute in the Set-Cookie header match the values used when the cookie was created.

== Server -> User Agent ==

Set-Cookie: lang=; Expires=Sun, 06 Nov 1994 08:49:37 GMT

== User Agent -> Server ==

Cookie: SID=31d4d96e407aad42

4. Server Requirements

This section describes the syntax and semantics of a well-behaved profile of the Cookie and Set-Cookie headers. Servers SHOULD limit themselves to the profile described in this section, both to maximize interoperability with existing user agents and because a future version of the Cookie or Set-Cookie headers could remove support for some of the esoteric semantics described in [Section 5 \(User Agent Requirements\)](#). User agents, however, MUST implement the requirements in [Section 5 \(User Agent Requirements\)](#) to ensure interoperability with servers making use of the full semantics.

4.1. Set-Cookie

[TOC](#)

The Set-Cookie HTTP response header is used to send cookies from the server to the user agent.

4.1.1. Syntax

[TOC](#)

Informally, the Set-Cookie response header contains the header name "Set-Cookie" followed by a ":" and a cookie. Each cookie begins with a name-value pair, followed by zero or more attribute-value pairs. Servers SHOULD NOT send Set-Cookie headers that fail to conform to the following grammar:


```

set-cookie-header = "Set-Cookie:" SP set-cookie-string
set-cookie-string = cookie-pair *( ";" SP cookie-av )
cookie-pair       = cookie-name "=" cookie-value
cookie-name       = token
cookie-value      = token
token             = <token, defined in [RFC2616], Section 2.2>

cookie-av         = expires-av / max-age-av / domain-av /
                  path-av / secure-av / httponly-av /
                  extension-av
expires-av        = "Expires=" sane-cookie-date
sane-cookie-date  = <rfc1123-date, defined in [RFC2616], Section 3.3.1>
max-age-av       = "Max-Age=" 1*DIGIT
domain-av        = "Domain=" domain-value
domain-value      = <subdomain>
                  ; defined in [RFC1034], Section 3.5, as
                  ; enhanced by [RFC1123], Section 2.1
path-av          = "Path=" path-value
path-value        = <any CHAR except CTLs or ";">
secure-av        = "Secure"
httponly-av      = "HttpOnly"
extension-av     = <any CHAR except CTLs or ";">

```

Note that some of the grammatical terms above reference documents that use different grammatical notations than this document (which uses ABNF from [\[RFC5234\] \(Crocker, D., Ed. and P. Overell, "Augmented BNF for Syntax Specifications: ABNF," January 2008.\)](#)).

The semantics of the cookie-value are not defined by this document. To maximize compatibility with user agents, servers that wish to store non-ASCII data in a cookie-value SHOULD encode that data using a printable ASCII encoding.

The portions of the set-cookie-string produced by the cookie-av term are known as attributes. To maximize compatibility with user agents, servers SHOULD NOT produce two attributes with the same name in the same set-cookie-string.

Servers SHOULD NOT include more than one Set-Cookie header field in the same response with the same cookie-name.

If a server sends multiple responses containing Set-Cookie headers concurrently to the user agent (e.g., when communicating with the user agent over multiple sockets), these responses create a "race condition" that can lead to unpredictable behavior.

NOTE: Some legacy user agents differ on their interpretation of two-digit years. To avoid compatibility issues, servers SHOULD use the rfc1123-date format, which requires a four-digit year.

NOTE: Some user agents represent dates using 32-bit UNIX `time_t` values. Some of these user agents might contain bugs that cause them to process dates after the year 2038 incorrectly.

4.1.2. Semantics (Non-Normative)

[TOC](#)

This section describes a simplified semantics of the Set-Cookie header. These semantics are detailed enough to be useful for understanding the most common uses of cookies by servers. The full semantics are described in [Section 5 \(User Agent Requirements\)](#).

When the user agent receives a Set-Cookie header, the user agent stores the cookie together with its attributes. Subsequently, when the user agent makes an HTTP request, the user agent includes the applicable, non-expired cookies in the Cookie header.

If the user agent receives a new cookie with the same cookie-name, domain-value, and path-value as a cookie that it has already stored, the existing cookie is evicted and replaced with the new cookie. Notice that servers can delete cookies by sending the user agent a new cookie with an Expires attribute with a value in the past.

Unless the cookie's attributes indicate otherwise, the cookie is returned only to the origin server, and it expires at the end of the current session (as defined by the user agent). User agents ignore unrecognized cookie attributes.

4.1.2.1. The Expires Attribute

[TOC](#)

The Expires attribute indicates the maximum lifetime of the cookie, represented as the date and time at which the cookie expires. The user agent is not required to retain the cookie until the specified date has passed. In fact, user agents often evict cookies due to memory pressure or privacy concerns.

4.1.2.2. The Max-Age Attribute

[TOC](#)

The Max-Age attribute indicates the maximum lifetime of the cookie, represented as the number of seconds until the cookie expires. The user agent is not required to retain the cookie for the specified duration. In fact, user agents often evict cookies from due to memory pressure or privacy concerns.

NOTE: Some legacy user agents do not support the Max-Age attribute. User agents that do not support the Max-Age attribute ignore the attribute.

If a cookie has both the Max-Age and the Expires attribute, the Max-Age attribute has precedence and controls the expiration date of the cookie. If a cookie has neither the Max-Age nor the Expires attribute, the user agent will retain the cookie until "the current session is over" (as defined by the user agent).

4.1.2.3. The Domain Attribute

[TOC](#)

The Domain attribute specifies those hosts to which the cookie will be sent. For example, if the value of the Domain attribute is "example.com", the user agent will include the cookie in the Cookie header when making HTTP requests to example.com, www.example.com, and www.corp.example.com. (Note that a leading %x2E ("."), if present, is ignored even though that character is not permitted.) If the server omits the Domain attribute, the user agent will return the cookie only to the origin server.

WARNING: Some legacy user agents treat an absent Domain attribute as if the Domain attribute were present and contained the current host name. For example, if example.com returns a Set-Cookie header without a Domain attribute, these user agents will erroneously send the cookie to www.example.com as well.

The user agent will reject cookies unless the Domain attribute specifies a scope for the cookie that would include the origin server. For example, the user agent will accept a cookie with a Domain attribute of "example.com" or of "foo.example.com" from foo.example.com, but the user agent will not accept a cookie with a Domain attribute of "bar.example.com" or of "baz.foo.example.com". NOTE: For security reasons, many user agents are configured to reject Domain attributes that correspond to "public suffixes." For example, some user agents will reject Domain attributes of "com" or "co.uk".

4.1.2.4. The Path Attribute

[TOC](#)

The scope of each cookie is limited to a set of paths, controlled by the Path attribute. If the server omits the Path attribute, the user agent will use the "directory" of the request-uri's path component as the default value. (See [Section 5.1.4 \(Paths and path-match\)](#) for more details.)

The user agent will include the cookie in an HTTP request only if the path portion of the request-uri matches (or is a subdirectory of) the cookie's Path attribute, where the %x2F ("/") character is interpreted as a directory separator.

Although seemingly useful for isolating cookies between different paths within a given host, the Path attribute cannot be relied upon for security (see [Section 8 \(Security Considerations\)](#)).

4.1.2.5. The Secure Attribute

[TOC](#)

The Secure attribute limits the scope of the cookie to "secure" channels (where "secure" is defined by the user agent). When a cookie has the Secure attribute, the user agent will include the cookie in an HTTP request only if the request is transmitted over a secure channel (typically HTTP over SSL, HTTP over TLS [\[RFC2818\] \(Rescorla, E., "HTTP Over TLS," May 2000.\)](#), and TLS [\[RFC5246\] \(Dierks, T. and E. Rescorla, "The Transport Layer Security \(TLS\) Protocol Version 1.2," August 2008.\)](#) itself).

Although seemingly useful for protecting cookies from active network attackers, the Secure attribute protects only the cookie's confidentiality. An active network attacker can overwrite Secure cookies from an insecure channel, disrupting their integrity (see [Section 8.6 \(Weak Integrity\)](#) for more details).

4.1.2.6. The HttpOnly Attribute

[TOC](#)

The HttpOnly attribute limits the scope of the cookie to HTTP requests. In particular, the attribute instructs the user agent to omit the cookie when providing access to cookies via "non-HTTP" APIs (such as a web browser API that exposes cookies to scripts).

4.2. Cookie

[TOC](#)

4.2.1. Syntax

[TOC](#)

The user agent sends stored cookies to the origin server in the Cookie header. If the server conforms to the requirements in [Section 4.1 \(Set-Cookie\)](#) (and the user agent conforms to the requirements in the

[Section 5 \(User Agent Requirements\)](#)), the user agent will send a Cookie header that conforms to the following grammar:

```
cookie-header = "Cookie:" OWS cookie-string OWS
cookie-string = cookie-pair *( ";" SP cookie-pair )
```

4.2.2. Semantics

[TOC](#)

Each cookie-pair represents a cookie stored by the user agent. The cookie-pair contains the cookie-name and cookie-value the user agent received in the Set-Cookie header.

Notice that the cookie attributes are not returned. In particular, the server cannot determine from the Cookie header alone when a cookie will expire, for which hosts the cookie is valid, for which paths the cookie is valid, or whether the cookie was set with the Secure or HttpOnly attributes.

The semantics of individual cookies in the Cookie header are not defined by this document. Servers are expected to imbue these cookies with application-specific semantics.

Although cookies are serialized linearly in the Cookie header, servers SHOULD NOT rely upon the serialization order. In particular, if the Cookie header contains two cookies with the same name (e.g., that were set with different Path or Domain attributes), servers SHOULD NOT rely upon the order in which these cookies appear in the header.

5. User Agent Requirements

[TOC](#)

For historical reasons, the full semantics of cookies (as presently deployed on the Internet) contain a number of exotic quirks. This section is intended to specify the Cookie and Set-Cookie headers in sufficient detail to allow a user agent implementing these requirements precisely to interoperate with existing servers.

5.1. Subcomponent Algorithms

[TOC](#)

This section defines some algorithms used by user agents to process specific subcomponents of the Cookie and Set-Cookie headers.

[TOC](#)

5.1.1. Dates

The user agent MUST use an algorithm equivalent to the following algorithm to parse a cookie-date. Note that the various boolean flags defined as a part of the algorithm are initially "not set".

1. Using the grammar below, divide the cookie-date into date-tokens.

```
cookie-date      = *delimiter date-token-list *delimiter
date-token-list = date-token *( 1*delimiter date-token )
date-token       = 1*non-delimiter

delimiter        = %x09 / %x20-2F / %x3B-40 / %x5B-60 / %x7B-7E
non-delimiter    = %x00-08 / %x0A-1F / DIGIT / ":" / ALPHA / %x7F-FF
non-digit        = %x00-2F / %x3A-FF

day-of-month     = 1*2DIGIT ( non-digit *OCTET )
month            = ( "jan" / "feb" / "mar" / "apr" /
                    "may" / "jun" / "jul" / "aug" /
                    "sep" / "oct" / "nov" / "dec" ) *OCTET
year             = 1*4DIGIT ( non-digit *OCTET )
time             = hms-time ( non-digit *OCTET )
hms-time         = time-field ":" time-field ":" time-field
time-field       = 1*2DIGIT
```

2. Process each date-token sequentially in the order the date-tokens appear in the cookie-date:
 1. If the found-time flag is not set and the token matches the time production, set the found-time flag and set the hour-value, minute-value, and second-value to the numbers denoted by the digits in the date-token, respectively. Skip the remaining sub-steps and continue to the next date-token.
 2. If the found-day-of-month flag is not set and the date-token matches the day-of-month production, set the found-day-of-month flag and set the day-of-month-value to the number denoted by the date-token. Skip the remaining sub-steps and continue to the next date-token.
 3. If the found-month flag is not set and the date-token matches the month production, set the found-month flag and set the month-value to the month denoted by the date-token. Skip the remaining sub-steps and continue to the next date-token.

4. If the found-year flag is not set and the date-token matches the year production, set the found-year flag and set the year-value to the number denoted by the date-token. Skip the remaining sub-steps and continue to the next date-token.
3. If the year-value is greater than or equal to 70 and less than or equal to 99, increment the year-value by 1900.
4. If the year-value is greater than or equal to 0 and less than or equal to 69, increment the year-value by 2000.
 1. NOTE: Some legacy user agents interpret two-digit years differently.
5. Abort these steps and fail to parse the cookie-date if
 - *at least one of the found-day-of-month, found-month, found-year, or found-time flags is not set,
 - *the day-of-month-value is less than 1 or greater than 31,
 - *the year-value is less than 1601,
 - *the hour-value is greater than 23,
 - *the minute-value is greater than 59, or
 - *the second-value is greater than 59.
6. Let the parsed-cookie-date be the date whose day-of-month, month, year, hour, minute, and second (in GMT) are the day-of-month-value, the month-value, the year-value, the hour-value, the minute-value, and the second-value, respectively. If no such date exists, abort these steps and fail to parse the cookie-date.
7. Return the parsed-cookie-date as the result of this algorithm.

5.1.2. Canonicalized host names

[TOC](#)

A canonicalized host name is the string generated by the following algorithm:

1. Convert the host name to a sequence of NR-LDH labels (see Section 2.3.2.2 of [\[RFC5890\] \(Klensin, J., "Internationalized Domain Names for Applications \(IDNA\): Definitions and Document](#)

[Framework," August 2010.\)\)](#) and/or A-labels according to the appropriate IDNA specification [\[RFC5891\] \(Klensin, J., "Internationalized Domain Names in Applications \(IDNA\): Protocol," August 2010.\)](#) or [\[RFC3490\] \(Faltstrom, P., Hoffman, P., and A. Costello, "Internationalizing Domain Names in Applications \(IDNA\)," March 2003.\)](#) (see [Section 6.3 \(IDNA dependency and migration\)](#) of this specification)

2. Convert the labels to lower case.
3. Concatenate the labels, separating each label from the next with a %x2E (".") character.

5.1.3. Domain matching

[TOC](#)

A string domain-matches a given domain string if at least one of the following conditions hold:

- *The domain string and the string are identical.
- *All of the following conditions hold:
 - The domain string is a suffix of the string.
 - The last character of the string that is not included in the domain string is a %x2E (".") character.
 - The string is a host name (i.e., not an IP address).

5.1.4. Paths and path-match

[TOC](#)

The user agent MUST use an algorithm equivalent to the following algorithm to compute the default-path of a cookie:

1. Let uri-path be the path portion of the request-uri if such a portion exists (and empty otherwise). For example, if the request-uri contains just a path (and optional query string), then the uri-path is that path (without the %x3F ("?") character or query string), and if the request-uri contains a full absoluteURI, the uri-path is the path component of that URI.

2. If the uri-path is empty or if first character of the uri-path is not a %x2F ("/") character, output %x2F ("/") and skip the remaining steps.
3. If the uri-path contains only a single %x2F ("/") character, output %x2F ("/") and skip the remaining steps.
4. Output the characters of the uri-path from the first character up to, but not including, the right-most %x2F ("/").

A request-path path-matches a given cookie-path if at least one of the following conditions hold:

- *The cookie-path and the request-path are identical.
- *The cookie-path is a prefix of the request-path and the last character of the cookie-path is %x2F ("/").
- *The cookie-path is a prefix of the request-path and the first character of the request-path that is not included in the cookie-path is a %x2F ("/") character.

5.2. The Set-Cookie Header

[TOC](#)

When a user agent receives a Set-Cookie header field in an HTTP response, the user agent MUST parse the field-value of the Set-Cookie header field as a set-cookie-string (defined below).

NOTE: The algorithm below is more permissive than the grammar in [Section 4.1 \(Set-Cookie\)](#). For example, the algorithm strips leading and trailing whitespace from the cookie name and value (but maintains internal whitespace), whereas the grammar in [Section 4.1 \(Set-Cookie\)](#) forbids whitespace in these positions. User agents use this algorithm so as to interoperate with servers that do not follow the recommendations in [Section 4 \(Server Requirements\)](#).

A user agent MUST use an algorithm equivalent to the following algorithm to parse a "set-cookie-string":

1. If the set-cookie-string contains a %x3B (";") character:

The name-value-pair string consists of the characters up to, but not including, the first %x3B (";"), and the unparsed-attributes consist of the remainder of the set-cookie-string (including the %x3B (";") in question).

Otherwise:

The name-value-pair string consists of all the characters contained in the set-cookie-string, and the unparsed-attributes is the empty string.

2. If the name-value-pair string lacks a %x3D ("=") character, ignore the set-cookie-string entirely.
3. The (possibly empty) name string consists of the characters up to, but not including, the first %x3D ("=") character, and the (possibly empty) value string consists of the characters after the first %x3D ("=") character.
4. Remove any leading or trailing WSP characters from the name string and the value string.
5. If the name string is empty, ignore the set-cookie-string entirely.
6. The cookie-name is the name string, and the cookie-value is the value string.

The user agent MUST use an algorithm equivalent to the following algorithm to parse the unparsed-attributes:

1. If the unparsed-attributes string is empty, skip the rest of these steps.
2. Discard the first character of the unparsed-attributes (which will be a %x3B (";") character).
3. If the remaining unparsed-attributes contains a %x3B (";") character:

Consume the characters of the unparsed-attributes up to, but not including, the first %x3B (";") character.

Otherwise:

Consume the remainder of the unparsed-attributes.

Let the cookie-av string be the characters consumed in this step.

4. If the cookie-av string contains a %x3D ("=") character:

The (possibly empty) attribute-name string consists of the characters up to, but not including, the first %x3D ("=") character, and the (possibly empty) attribute-value string consists of the characters after the first %x3D ("=") character.

Otherwise:

The attribute-name string consists of the entire cookie-av string, and the attribute-value string is empty.

5. Remove any leading or trailing WSP characters from the attribute-name string and the attribute-value string.
6. Process the attribute-name and attribute-value according to the requirements in the following subsections. (Notice that attributes with unrecognized attribute-names are ignored.)
7. Return to Step 1 of this algorithm.

When the user agent finishes parsing the set-cookie-string, the user agent is said to "receive a cookie" from the request-uri with name cookie-name, value cookie-value, and attributes cookie-attribute-list. (See [Section 5.3 \(Storage Model\)](#) for additional requirements triggered by receiving a cookie.)

5.2.1. The Expires Attribute

[TOC](#)

If the attribute-name case-insensitively matches the string "Expires", the user agent MUST process the cookie-av as follows.

Let the expiry-time be the result of parsing the attribute-value as cookie-date (see [Section 5.1.1 \(Dates\)](#)).

If the attribute-value failed to parse as a cookie date, ignore the cookie-av.

If the expiry-time is later than the last date the user agent can represent, the user agent MAY replace the expiry-time with the last representable date.

If the expiry-time is earlier than the earliest date the user agent can represent, the user agent MAY replace the expiry-time with the earliest representable date.

Append an attribute to the cookie-attribute-list with an attribute-name of Expires and an attribute-value of expiry-time.

5.2.2. The Max-Age Attribute

[TOC](#)

If the attribute-name case-insensitively matches the string "Max-Age", the user agent MUST process the cookie-av as follows.

If the first character of the attribute-value is not a DIGIT or a "-" character, ignore the cookie-av.

If the remainder of attribute-value contains a non-DIGIT character, ignore the cookie-av.
Let delta-seconds be the attribute-value converted to an integer.
If delta-seconds is less than or equal to zero (0), let expiry-time be the earliest representable date and time. Otherwise, let the expiry-time be the current date and time plus delta-seconds seconds.
Append an attribute to the cookie-attribute-list with an attribute-name of Max-Age and an attribute-value of expiry-time.

5.2.3. The Domain Attribute

[TOC](#)

If the attribute-name case-insensitively matches the string "Domain", the user agent MUST process the cookie-av as follows.
If the attribute-value is empty, the behavior is undefined. However, user agent SHOULD ignore the cookie-av entirely.
If the first character of the attribute-value string is %x2E ("."):

Let cookie-domain be the attribute-value without the leading %x2E (".") character.

Otherwise:

Let cookie-domain be the entire attribute-value.

Convert the cookie-domain to lower case.
Append an attribute to the cookie-attribute-list with an attribute-name of Domain and an attribute-value of cookie-domain.

5.2.4. The Path Attribute

[TOC](#)

If the attribute-name case-insensitively matches the string "Path", the user agent MUST process the cookie-av as follows.
If the attribute-value is empty or if the first character of the attribute-value is not %x2F ("/"):

Let cookie-path be the default-path.

Otherwise:

Let cookie-path be the attribute-value.

Append an attribute to the cookie-attribute-list with an attribute-name of Path and an attribute-value of cookie-path.

5.2.5. The Secure Attribute

[TOC](#)

If the attribute-name case-insensitively matches the string "Secure", the user agent MUST append an attribute to the cookie-attribute-list with an attribute-name of Secure and an empty attribute-value.

5.2.6. The HttpOnly Attribute

[TOC](#)

If the attribute-name case-insensitively matches the string "HttpOnly", the user agent MUST append an attribute to the cookie-attribute-list with an attribute-name of HttpOnly and an empty attribute-value.

5.3. Storage Model

[TOC](#)

The user agent stores the following fields about each cookie: name, value, expiry-time, domain, path, creation-time, last-access-time, persistent-flag, host-only-flag, secure-only-flag, and http-only-flag. When the user agent "receives a cookie" from a request-uri with name cookie-name, value cookie-value, and attributes cookie-attribute-list, the user agent MUST process the cookie as follows:

1. A user agent MAY ignore a received cookie in its entirety. For example, the user agent might wish to block receiving cookies from "third-party" responses or the user agent might not wish to store cookies that exceed some size.
2. Create a new cookie with name cookie-name, value cookie-value. Set the creation-time and the last-access-time to the current date and time.
3. If the cookie-attribute-list contains an attribute with an attribute-name of "Max-Age":

Set the cookie's persistent-flag to true.

Set the cookie's expiry-time to attribute-value of the last attribute in the cookie-attribute-list with an attribute-name of "Max-Age".

Otherwise, if the cookie-attribute-list contains an attribute with an attribute-name of "Expires" (and does not contain an attribute with an attribute-name of "Max-Age"):

Set the cookie's persistent-flag to true.

Set the cookie's expiry-time to attribute-value of the last attribute in the cookie-attribute-list with an attribute-name of "Expires".

Otherwise:

Set the cookie's persistent-flag to false.

Set the cookie's expiry-time to the latest representable date.

4. If the cookie-attribute-list contains an attribute with an attribute-name of "Domain":

Let the domain-attribute be the attribute-value of the last attribute in the cookie-attribute-list with an attribute-name of "Domain".

Otherwise:

Let the domain-attribute be the empty string.

5. If the user agent is configured to reject "public suffixes" and the domain-attribute is a public suffix:

If the domain-attribute is identical to the canonicalized request-host:

Let the domain-attribute be the empty string.

Otherwise:

Ignore the cookie entirely and abort these steps

NOTE: A "public suffix" is a domain that is controlled by a public registry, such as "com", "co.uk", and "pvt.k12.wy.us". This step is essential for preventing attacker.com from disrupting the integrity of example.com by setting a cookie with a Domain attribute of "com". Unfortunately, the set of public suffixes (also known as "registry controlled domains") changes over time. If feasible, user agents SHOULD use an up-to-date public suffix list, such as the one maintained by the Mozilla project at <http://publicsuffix.org/>.

6. If the domain-attribute is non-empty:

If the canonicalized request-host does not domain-match the domain-attribute, ignore the cookie entirely and abort these steps.

Set the cookie's host-only-flag to false.

Set the cookie's domain to the domain-attribute.

Otherwise:

Set the cookie's host-only-flag to true.

Set the cookie's domain to the canonicalized request-host.

7. If the cookie-attribute-list contains an attribute with an attribute-name of "Path", set the cookie's path to attribute-value of the last attribute in the cookie-attribute-list with an attribute-name of "Path". Otherwise, set cookie's path to the default-path of the request-uri.
8. If the cookie-attribute-list contains an attribute with an attribute-name of "Secure", set the cookie's secure-only-flag to true. Otherwise, set cookie's secure-only-flag to false.
9. If the cookie-attribute-list contains an attribute with an attribute-name of "HttpOnly", set the cookie's http-only-flag to true. Otherwise, set cookie's http-only-flag to false.
10. If the cookie was received from a "non-HTTP" API and the cookie's http-only-flag is set, abort these steps and ignore the cookie entirely.
11. If the cookie store contains a cookie with the same name, domain, and path as the newly created cookie:
 1. Let old-cookie be the existing cookie with the same name, domain, and path as the newly created cookie. (Notice that this algorithm maintains the invariant that there is at most one such cookie.)
 2. If the newly created cookie was received from an "non-HTTP" API and the old-cookie's http-only-flag is set, abort these steps and ignore the newly created cookie entirely.
 3. Update the creation-time of the newly created cookie to match the creation-time of the old-cookie.
 4. Remove the old-cookie from the cookie store.
12. Insert the newly created cookie into the cookie store.

A cookie is "expired" if the cookie has an expiry date in the past.

The user agent MUST evict all expired cookies from the cookie store if, at any time, an expired cookie exists in the cookie store.

At any time, the user agent MAY "remove excess cookies" from the cookie store if the number of cookies sharing a domain field exceeds some implementaiton defined upper bound (such as 50 cookies).

At any time, the user agent MAY "remove excess cookies" from the cookie store if the cookie store exceeds some predetermined upper bound (such as 3000 cookies).

When the user agent removes excess cookies from the cookie store, the user agent MUST evict cookies in the following priority order:

1. Expired cookies.
2. Cookies that share a domain field with more than a predetermined number of other cookies.
3. All cookies.

If two cookies have the same removal priority, the user agent MUST evict the cookie with the earliest last-access date first.

When "the current session is over" (as defined by the user agent), the user agent MUST remove from the cookie store all cookies with the persistent-flag set to false.

5.4. The Cookie Header

[TOC](#)

The user agent includes stored cookies in the Cookie HTTP request header.

When the user agent generates an HTTP request, the user agent MUST NOT attach more than one Cookie header field.

A user agent MAY omit the Cookie header in its entirety. For example, the user agent might wish to block sending cookies during "third-party" requests.

If the user agent does attach a Cookie header field to an HTTP request, the user agent MUST send the cookie-string (defined below) as the value of the header field.

The user agent MUST use an algorithm equivalent to the following algorithm to compute the "cookie-string" from a cookie store and a request-uri:

1. Let cookie-list be the set of cookies from the cookie store that meet all of the following requirements:

*Either:

The cookie's host-only-flag is true and the canonicalized request-host is identical to the cookie's domain.

Or:

The cookie's host-only-flag is false and the canonicalized request-host domain-matches cookie's domain.

*The request-uri's path path-matches cookie's path.

*If the cookie's secure-only-flag is true, then the request-uri's scheme must denote a "secure" protocol (as defined by the user agent).

NOTE: The notion of a "secure" protocol is not defined by this document. Typically, user agents consider a protocol secure if the protocol makes use of transport-layer security, such as SSL or TLS. For example, most user agents consider "https" to be a scheme that denotes a secure protocol.

*If the cookie's http-only-flag is true, then exclude the cookie if the cookie-string is being generated for a "non-HTTP" API (as defined by the user agent).

2. The user agent SHOULD sort the cookie-list in the following order:

*Cookies with longer paths are listed before cookies with shorter paths.

*Among cookies that have equal length path fields, cookies with earlier creation-times are listed before cookies with later creation-times.

NOTE: Not all user agents sort the cookie-list in this order, but this order reflects common practice when this document was written, and, historically, there have been servers that (erroneously) depended on this order.

3. Update the last-access-time of each cookie in the cookie-list to the current date and time.

4. Serialize the cookie-list into a cookie-string by processing each cookie in the cookie-list in order:

1. Output the cookie's name, the %x3D ("=") character, and the cookie's value.

2. If there is an unprocessed cookie in the cookie-list, output the characters %x3B and %x20 ("; ").

NOTE: Despite its name, the cookie-string is actually a sequence of octets, not a sequence of characters. To convert the cookie-string (or components thereof) into a sequence of characters (e.g., for presentation to the user), the user agent might wish use the UTF-8 character encoding [\[RFC3629\] \(Yergeau, F., "UTF-8, a transformation format of ISO 10646," November 2003.\)](#) to decode the octet sequence.

6. Implementation Considerations

[TOC](#)

6.1. Limits

[TOC](#)

Practical user agent implementations have limits on the number and size of cookies that they can store. General-use user agents SHOULD provide each of the following minimum capabilities:

- *At least 4096 bytes per cookie (as measured by the sum of the length of the cookie's name, value, and attributes).

- *At least 50 cookies per domain.

- *At least 3000 cookies total.

Servers SHOULD use as few and as small cookies as possible to avoid reaching these implementation limits and to minimize network bandwidth due to the Cookie header being included in every request. Servers SHOULD gracefully degrade if the user agent fails to return one or more cookies in the Cookie header because the user agent might evict any cookie at any time on orders from the user.

6.2. Application Programming Interfaces

[TOC](#)

One reason the Cookie and Set-Cookie headers uses such esoteric syntax is because many platforms (both in servers and user agents) provide a string-based application programming interface (API) to cookies, requiring application-layer programmers to generate and parse the syntax used by the Cookie and Set-Cookie headers, which many programmers have done incorrectly, resulting in interoperability problems.

Instead of providing string-based APIs to cookies, platforms would be well-served by providing more semantic APIs. It is beyond the scope of this document to recommend specific API designs, but there are clear

benefits to accepting an abstract "Date" object instead of a serialized date string.

6.3. IDNA dependency and migration

[TOC](#)

IDNA2008 [\[RFC5890\]](#) (Klensin, J., "Internationalized Domain Names for Applications (IDNA): Definitions and Document Framework," August 2010.) supersedes IDNA2003 [\[RFC3490\]](#) (Faltstrom, P., Hoffman, P., and A. Costello, "Internationalizing Domain Names in Applications (IDNA)," March 2003.) but is not backwards-compatible. For this reason, there will be a transition period (possibly of a number of years). User agents SHOULD implement IDNA2008 [\[RFC5890\]](#) (Klensin, J., "Internationalized Domain Names for Applications (IDNA): Definitions and Document Framework," August 2010.) and MAY implement [Unicode Technical Standard #46 <<http://unicode.org/reports/tr46/>>] in order to facilitate a smoother IDNA transition. If a user agent does not implement IDNA2008, the user agent MUST implement IDNA2003 [\[RFC3490\]](#) (Faltstrom, P., Hoffman, P., and A. Costello, "Internationalizing Domain Names in Applications (IDNA)," March 2003.).

7. Privacy Considerations

[TOC](#)

Cookies are often criticized for letting servers track users. For example, a number of "web analytics" companies use cookies to recognize when a user returns to a web site or visits another web site. Although cookies are not the only mechanism servers can use to track users across HTTP requests, cookies facilitate tracking because they are persistent across user agent sessions and can be shared between hosts.

7.1. Third-Party Cookies

[TOC](#)

Particularly worrisome are so-called "third-party" cookies. In rendering an HTML document, a user agent often requests resources from other servers (such as advertising networks). These third-party servers can use cookies to track the user even if the user never visits the server directly.

Some user agents restrict how third-party cookies behave. For example, some of these user agents refuse to send the Cookie header in third-party requests. Others refuse to process the Set-Cookie header in responses to third-party requests. User agents vary widely in their third-party cookie policies. This document grants user agents wide

latitude to experiment with third-party cookie policies that balance the privacy and compatibility needs of their users. However, this document does not endorse any particular third-party cookie policy. Third-party cookie blocking policies are often ineffective at achieving their privacy goals if servers attempt to work around their restrictions to track users. In particular, two collaborating servers can often track users without using cookies at all.

7.2. User Controls

[TOC](#)

User agents should provide users with a mechanism for managing the cookies stored in the cookie store. For example, a user agent might let users delete all cookies received during a specified time period or all the cookies related to a particular domain. In addition, many user agent include a user interface element that lets users examine the cookies stored in their cookie store.

User agents should provide users with a mechanism for disabling cookies. When cookies are disabled, the user agent **MUST NOT** include a Cookie header in outbound HTTP requests and the user agent **MUST NOT** process Set-Cookie headers in inbound HTTP responses.

Some user agents provide users the option of preventing persistent storage of cookies across sessions. When configured thusly, user agents **MUST** treat all received cookies as if the persistent-flag were set to false.

Some user agents provide users with the ability to approve individual writes to the cookie store. In many common usage scenarios, these controls generate a large number of prompts. However, some privacy-conscious users find these controls useful nonetheless.

8. Security Considerations

[TOC](#)

8.1. Overview

[TOC](#)

Cookies have a number of security pitfalls. This section overviews a few of the more salient issues.

In particular, cookies encourage developers to rely on ambient authority for authentication, often becoming vulnerable to attacks such as cross-site request forgery. Also, when storing session identifiers in cookies, developers often create session fixation vulnerabilities.

Transport-layer encryption, such as that employed in HTTPS, is insufficient to prevent a network attacker from obtaining or altering a victim's cookies because the cookie protocol itself has various vulnerabilities (see "Weak Confidentiality" and "Weak Integrity", below). In addition, by default, cookies do not provide confidentiality or integrity from network attackers, even when used in conjunction with HTTPS.

8.2. Ambient Authority

[TOC](#)

A server that uses cookies to authenticate users can suffer security vulnerabilities because some user agents let remote parties issue HTTP requests from the user agent (e.g., via HTTP redirects or HTML forms). When issuing those requests, user agents attach cookies even if the remote party does not know the contents of the cookies, potentially letting the remote party exercise authority at an unwary server. Although this security concern goes by a number of names (e.g., cross-site request forgery, confused deputy), the issue stems from cookies being a form of ambient authority. Cookies encourage server operators to separate designation (in the form of URLs) from authorization (in the form of cookies). Consequently, the user agent might supply the authorization for a resource designated by the attacker, possibly causing the server or its clients to undertake actions designated by the attacker as though they were authorized by the user. Instead of using cookies for authorization, server operators might wish to consider entangling designation and authorization by treating URLs as capabilities. Instead of storing secrets in cookies, this approach stores secrets in URLs, requiring the remote entity to supply the secret itself. Although this approach is not a panacea, judicious application of these principles can lead to more robust security.

8.3. Clear Text

[TOC](#)

Unless sent over a secure channel (such as TLS), the information in the Cookie and Set-Cookie headers is transmitted in the clear.

1. All sensitive information conveyed in these headers is exposed to an eavesdropper.
2. A malicious intermediary could alter the headers as they travel in either direction, with unpredictable results.
3. A malicious client could alter the Cookie header before transmission, with unpredictable results.

Servers SHOULD encrypt and sign the contents of cookies when transmitting them to the user agent (even when sending the cookies over a secure channel). However, encrypting and signing cookie contents does not prevent an attacker from transplanting a cookie from one user agent to another or from replaying the cookie at a later time.

In addition to encrypting and signing the contents of every cookie, servers that require a higher level of security SHOULD use the Cookie and Set-Cookie headers only over a secure channel. When using cookies over a secure channel, servers SHOULD set the Secure attribute (see [Section 4.1.2.5 \(The Secure Attribute\)](#)) for every cookie. If a server does not set the Secure attribute, the protection provided by the secure channel will be largely moot.

8.4. Session Identifiers

[TOC](#)

Instead of storing session information directly in a cookie (where it might be exposed to or replayed by an attacker), servers commonly store a nonce (or "session identifier") in a cookie. When the server receives an HTTP request with a nonce, the server can look up state information associated with the cookie using the nonce as a key.

Using session identifier cookies limits the damage an attacker can cause if the attacker learns the contents of a cookie because the nonce is useful only for interacting with the server (unlike non-nonce cookie content, which might itself be sensitive). Furthermore, using a single nonce prevents an attacker from "splicing" together cookie content from two interactions with the server, which could cause the server to behave unexpectedly.

Using session identifiers is not without risk. For example, the server SHOULD take care to avoid "session fixation" vulnerabilities. A session fixation attack proceeds in three steps. First, the attacker transplants a session identifier from his or her user agent to the victim's user agent. Second, the victim uses that session identifier to interact with the server, possibly imbuing the session identifier with the user's credentials or confidential information. Third, the attacker uses the session identifier to interact with server directly, possibly obtaining the user's authority or confidential information.

8.5. Weak Confidentiality

[TOC](#)

Cookies do not provide isolation by port. If a cookie is readable by a service running on one port, the cookie is also readable by a service running on another port of the same server. If a cookie is writable by a service on one port, the cookie is also writable by a service running on another port of the same server. For this reason, servers SHOULD NOT

both run mutually distrusting services on different ports of the same host and use cookies to store security-sensitive information. Cookies do not provide isolation by scheme. Although most commonly used with the http and https schemes, the cookies for a given host might also be available to other schemes, such as ftp and gopher. Although this lack of isolation by scheme is most apparent in non-HTTP APIs that permit access to cookies (e.g., HTML's document.cookie API), the lack of isolation by scheme is actually present in requirements for processing cookies themselves (e.g., consider retrieving a URI with the gopher scheme via HTTP). Cookies do not always provide isolation by path. Although the network-level protocol does not send cookies stored for one path to another, some user agents expose cookies via non-HTTP APIs, such as HTML's document.cookie API. Because some of these user agents (e.g., web browsers) do not isolate resources received from different paths, a resource retrieved from one path might be able to access cookies stored for another path.

8.6. Weak Integrity

[TOC](#)

Cookies do not provide integrity guarantees for sibling domains (and their subdomains). For example, consider foo.example.com and bar.example.com. The foo.example.com server can set a cookie with a Domain attribute of "example.com" (possibly overwriting an existing "example.com" cookie set by bar.example.com), and the user agent will include that cookie in HTTP requests to bar.example.com. In the worst case, bar.example.com will be unable to distinguish this cookie from a cookie it set itself. The foo.example.com server might be able to leverage this ability to mount an attack against bar.example.com. Even though the Set-Cookie header supports the Path attribute, the Path attribute does not provide any integrity protection because the user agent will accept an arbitrary Path attribute in a Set-Cookie header. For example, an HTTP response to a request for http://example.com/foo/bar can set a cookie with a Path attribute of "/qux". Consequently, servers SHOULD NOT both run mutually distrusting services on different paths of the same host and use cookies to store security-sensitive information.

An active network attacker can also inject cookies into the Cookie header sent to https://example.com/ by impersonating a response from http://example.com/ and injecting a Set-Cookie header. The HTTPS server at example.com will be unable to distinguish these cookies from cookies that it set itself in an HTTPS response. An active network attacker might be able to leverage this ability to mount an attack against example.com even if example.com uses HTTPS exclusively.

Servers can partially mitigate these attacks by encrypting and signing the contents of their cookies. However, using cryptography does not

mitigate the issue completely because an attacker can replay a cookie he or she received from the authentic example.com server in the user's session, with unpredictable results.

Finally, an attacker might be able to force the user agent to delete cookies by storing a large number of cookies. Once the user agent reaches its storage limit, the user agent will be forced to evict some cookies. Servers SHOULD NOT rely upon user agents retaining cookies.

8.7. Reliance on DNS

[TOC](#)

Cookies rely upon the Domain Name System (DNS) for security. If the DNS is partially or fully compromised, the cookie protocol might fail to provide the security properties required by applications.

9. IANA Considerations

[TOC](#)

The permanent message header field registry (see [\[RFC3864\] \(Klyne, G., Nottingham, M., and J. Mogul, "Registration Procedures for Message Header Fields," September 2004.\)](#)) should be updated with the following registrations:

9.1. Cookie

[TOC](#)

Header field name: Cookie

Applicable protocol: http

Status: standard

Author/Change controller: IETF

Specification document: this specification ([Section 5.4 \(The Cookie Header\)](#))

9.2. Set-Cookie

[TOC](#)

Header field name: Set-Cookie

Applicable protocol: http

Status: standard

Author/Change controller: IETF

Specification document: this specification ([Section 5.2 \(The Set-Cookie Header\)](#))

10. References

[TOC](#)

10.1. Normative References

[TOC](#)

[RFC1034]	Mockapetris, P., " Domain names - concepts and facilities ," STD 13, RFC 1034, November 1987 (TXT).
[RFC1123]	Braden, R., " Requirements for Internet Hosts - Application and Support ," STD 3, RFC 1123, October 1989 (TXT).
[RFC2119]	Bradner, S., " Key words for use in RFCs to Indicate Requirement Levels ," BCP 14, RFC 2119, March 1997 (TXT , HTML , XML).
[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.
[RFC3490]	Faltstrom, P., Hoffman, P., and A. Costello, " Internationalizing Domain Names in Applications (IDNA) ," RFC 3490, March 2003 (TXT). See Section 6.3 (IDNA dependency and migration) for an explanation why the normative reference to an obsoleted specification is needed.
[RFC3629]	Yergeau, F., " UTF-8, a transformation format of ISO 10646 ," STD 63, RFC 3629, November 2003 (TXT).
[RFC4790]	Newman, C., Duerst, M., and A. Gulbrandsen, " Internet Application Protocol Collation Registry ," RFC 4790, March 2007 (TXT).
[RFC5234]	Crocker, D., Ed. and P. Overell, " Augmented BNF for Syntax Specifications: ABNF ," STD 68, RFC 5234, January 2008.
[RFC5246]	Dierks, T. and E. Rescorla, " The Transport Layer Security (TLS) Protocol Version 1.2 ," RFC 5246, August 2008.
[RFC5890]	Klensin, J., " Internationalized Domain Names for Applications (IDNA): Definitions and Document Framework ," RFC 5890, August 2010 (TXT).
[RFC5891]	Klensin, J., " Internationalized Domain Names in Applications (IDNA): Protocol ," RFC 5891, August 2010 (TXT).

10.2. Informative References

[TOC](#)

[RFC2109]	Kristol, D. and L. Montulli , " HTTP State Management Mechanism ," RFC 2109, February 1997.
-----------	---

[RFC2965]	Kristol, D. and L. Montulli , " HTTP State Management Mechanism ," RFC 2965, October 2000.
[RFC2818]	Rescorla, E., " HTTP Over TLS ," RFC 2818, May 2000 (TXT).
[Netscape]	Netscape Communications Corp., " Persistent Client State -- HTTP Cookies ," 1999.
[Kri2001]	Kristol, D., " HTTP Cookies: Standards, Privacy, and Politics ," ACM Transactions on Internet Technology Vol. 1, #2, November 2001.
[RFC3864]	Klyne, G., Nottingham, M., and J. Mogul, " Registration Procedures for Message Header Fields ," BCP 90, RFC 3864, September 2004.

Appendix A. Acknowledgements

[TOC](#)

This document borrows heavily from RFC 2109 [[RFC2109](#)] ([Kristol, D. and L. Montulli](#), "[HTTP State Management Mechanism](#)," February 1997.). We are indebted to David M. Kristol and Lou Montulli for their efforts to specify cookies. David M. Kristol, in particular, provided invaluable advice on navigating the IETF process. We would also like to thank Thomas Broyer, Tyler Close, Bil Corry, corvid, Lisa Dusseault, Roy T. Fielding, Blake Frantz, Anne van Kesteren, Eran Hammer-Lahav, Jeff Hodges, Bjoern Hoehrmann, Achim Hoffmann, Georg Koppen, Dean McNamee, Mark Miller, Mark Pauley, Yngve N. Pettersen, Julian Reschke, Peter Saint-Andre, Mark Seaborn, Maciej Stachowiak, Daniel Stenberg, Tatsuhiro Tsujikawa, David Wagner, Dan Winship, and Dan Witte for their valuable feedback on this document.

Author's Address

[TOC](#)

	Adam Barth
	University of California, Berkeley
Email:	abarth@eecs.berkeley.edu
URI:	http://www.adambarth.com/