INTERNET-DRAFT
Intended Status: Informational

Stefan Santesson (Microsoft)
Kevin Damour (Microsoft)
Phil Hallin (Microsoft)

Expires January 2009

July 2008

Channel binding for HTTP Digest Authentication
<draft-santesson-digestbind-01.txt>

Status of this Memo

Abstract

This document specifies a method implemented by Microsoft to add channel binding capabilities to the http digest protocol defined in RFC 2617 [2617]

1. Introduction

This specification document Microsoft's existing implementation of TLS endpoint channel binding and service binding for http digest Authentication.

The primary purpose of this feature is to safeguard resources against authentication forwarding attacks.

Authentication forwarding is possible when http digest authentication takes place inside an outer secure channel (e.g. TLS). In this case, there is no binding between the inner channel session key and the outer channel session key. This specification defines a way to exchange necessary channel binding data for the outer channel within http digest authentication.

This specification expands the defined set of authentication parameters defined in RFC 2617 [2617] for the Authorization request header, when used with digest authentication. The semantics of server and client nonce are expanded to facilitate negotiation of channel binding.

1.1 Terminology

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 RFC 2119 [2119].

2. Protocol syntax

Channel binding is provided through amendments to the WWW-Authenticate Response Header sent by the server and the Authorization Request Header returned by the client, both defined in RFC 2616 [2616].

Authentication parameters (directives) defined in this specification, are defined within the auth-param syntax defined in RFC 2617 [2617]:

```
auth-param     = token "=" ( token | quoted-string )
```

2.1 WWW-Authenticate Response Header

The WWW-Authenticate Response Header sent by the server MUST be formed according to RFC 2617 [2617] section 3.2.1, with the amendments specified in this section.

nonce
A server signals that it supports channel binding according to this specification by invoking the following 12 characters in the server nonce:

"+UpGrAdEd+v1"

As the nonce directive is present, the qop-options directive MUST be present according to RFC 2617 [2617].

This specification only supports channel binding when the outer channel is TLS.

2.2 Authorization Request Header

The Authorization Request header sent by the client MUST be formed according to RFC 2617 [2617] section 3.2.2, with the amendments specified in this section.

digest-response is expanded with the following directives:

```
hashed-directives  = "hashed-dirs" "=" <"> 1#token <">
service-name       = "service-name" "=" service-name-value
charset            = "charset" "=" "utf-8"
channel-binding    = <"> 32LHEX <">
```

service-name-value is further defined as:

```
service-name-value = serv-type "/" host [ "/" serv-name ]
serv-type          = 1*ALPHA
host               = 1*( ALPHA | DIGIT | "-" | "." )
serv-name          = host
```

Definition of directive values:

cnonce
On the client side, an upgraded client recognizes the leading "+UpGrAdEd+v1" string in the server nonce and interprets it to mean that the server understands channel bindings according to this specification. This extends the semantics from RFC 2617 [2617] where the nonce is defined to be opaque to the client, but now conveys information from the server. If the client decides to send channel binding information, it includes the same "+UpGrAdEd+v1" prefix string at the beginning of the cnonce it generates. The MD5 ASCII hex of the unquoted service-name and channel-bindings directive values follows the upgraded prefix.

NOTE: Many existing client implementations ignores the "v1" part of the "+UpGrAdEd+v1" string and would not notice the difference if the string ended with "v2". This should be taken into consideration if a version 2 of this protocol is defined.

hashed-directives
The names of the directives, which values are hashed and included in the cnonce, provided as a quoted coma separated list. For version 1 (v1) of this specification, this directive MUST contain the following value:

hashed-dirs = "service-name,channel-binding"

service-name
The service-name directive is defined identically as the digest-uri directive of RFC 2831 [2831]. All conventions defined for the digest-uri directive in RFC 2831 apply also to this directive.

charset
This directive, if present, specifies that the server supports UTF-8 encoding for the username and password. This directive and conventions for its use are defined in RFC 2831 [2831].

channel-binding
This directive carries the octets of a channel binding token as defined in the IANA registry for Channel Binding Types, defined under RFC 5056 [5056]. The selected channel binding type for implementations of this specification MUST be "tls-server-end-point"

3 IANA Considerations

TBD

4 Security Considerations

TBD

5 References

5.1 Normative References

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

[2616] R. Fielding, J. Gettys, J. Mogul, H. Frystyk, L. Masinter, P. Leach, T. Berners-Lee, "Hypertext Transfer Protocol -- HTTP/1.1", RFC 2616, June 1999.

[2617] J. Franks, P. Hallam-Baker, J. Hostetler, S. Lawrence, P. Leach, A. Luotonen, L. Stewart, "HTTP Authentication: Basic and Digest Access Authentication", RFC 2617, June 1999.

[2831] P. Leach, C. Newman, "Using Digest Authentication as a SASL Mechanism", RFC 2831, May 2000.

[5056] N. Williams, "On the Use of Channel Bindings to Secure Channels", RFC 5056, November 2007.

5.2 Informative References

No informative references are listed.

Appendix A - Example

This is an example of a valid Authorization request header according to this specification:

```
Authorization : Digest
username="administrator",
realm="jeremyv-dom2.nttest.example.com",
nonce="+UpGrAdEd+v137576ac1877be8fe5993f505e48dc801d89a9e0a3e430
9b4dd10177754546bf5db46ee3b77fcb6317f569396da0b53fa",
uri="/dir/index.html",
cnonce="+UpGrAdEd+v19f74f856d6b97542776f92fa6d6f3429eb5ffa78b385
313f954e9f2226246bd9",
nc=00000001,
algorithm=MD5-sess,
response="5da37a37d5b3867366f22133182f1ef4",
qop="auth",
charset=utf-8,
hashed-dirs="service-name,channel-binding",
service-name="TestServiceName/example.com",
channel-binding="8674d6ce56be991be9c7549735f179f4"
```

Editorial note: This example will be updated. It is syntactically correct, but some hash values are not reflecting the actual values in the example.

Authors' Addresses

Stefan Santesson
Microsoft
One Microsoft Way
Redmond, WA 98052
USA

EMail: stefans(at)microsoft.com

Kevin Damour
Microsoft
One Microsoft Way
Redmond, WA 98052
USA

EMail: kdamour(at)microsoft.com

Phil Hallin
Microsoft
One Microsoft Way
Redmond, WA 98052
USA

EMail: philh(at)microsoft.com

Intellectual Property