User Session Tracking in RADIUS

draft-zorn-radius-logoff-02.txt

Status of this Memo

This document is an Internet-Draft and is in full conformance with all provisions of Section 10 of RFC2026.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

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."

The list of current Internet-Drafts can be accessed at http://www.ietf.org/ietf/1id-abstracts.txt.

The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html.

This Internet-Draft will expire on November 11, 2004.

Copyright Notice

Copyright (C) The Internet Society (2004). All Rights Reserved.

Abstract

This document defines a pair of new messages and a new attribute designed to allow RADIUS servers to cleanly track user sessions.
Table of Contents

1. Introduction ........................................... 3
2. Specification of Requirements .......................... 3
3. Packet Format ........................................... 3
4. Packet Types ........................................... 6
   4.1 User-Logoff-Notification ............................ 6
   4.2 User-Logoff-Acknowledgement ....................... 8
5. Attributes .............................................. 9
   5.1 Session-Id ........................................... 9
6. IANA Considerations ..................................... 10
7. Security Considerations ................................. 10
8. References .............................................. 10
   8.1 Normative References ................................. 10
   8.2 Informative References ............................... 11
   Author’s Address ........................................ 11
   Intellectual Property and Copyright Statements ........ 12
1. Introduction

RFC 2865 defines a "session" as a service provided to a user with the beginning of the session defined as the point where service is first provided and the end of the session defined as the point where service is ended. For authorization purposes, the beginning of a session Many remote access deployments require the tracking/counting of user sessions, for example to limit the number of simultaneous logins. Note that this is explicitly an authorization issue. Currently, however, the only way to track the number or even the existence of user sessions is via RADIUS Accounting [RFC2866]. This fact causes an unnecessarily tight binding between RADIUS [RFC2865] and RADIUS Accounting, forcing implementers to combine both protocols in a single server, devise a method to quickly search accounting logs, etc. and service providers to implement RADIUS Accounting even if they would not otherwise do so.

This document defines a message exchange that can be used to notify a RADIUS server that a user session has terminated.

Discussion of this draft may be directed to the author.

2. Specification of Requirements

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].

3. Packet Format

Exactly one RADIUS packet is encapsulated in the UDP Data field [RFC0768] where the UDP Destination Port field indicates 1812 (decimal).

When a reply is generated, the source and destination ports are reversed.

A summary of the RADIUS data format is shown below. The fields are transmitted from left to right.
Code

The Code field is one octet, and identifies the type of RADIUS packet. When a packet is received with an invalid Code field, it is silently discarded.

The RADIUS Codes (decimal) defined in this document are as follows:

<MSG1> User-Logoff-Notification
<MSG2> User-Logoff-Acknowledgement

Identifier

The Identifier field is one octet, and aids in matching requests and replies. The RADIUS server can detect a duplicate request if it has the same client source IP address, source UDP port and Identifier within a short span of time.

Length

The Length field is two octets. It indicates the length of the packet including the Code, Identifier, Length, Authenticator and Attribute fields. Octets outside the range of the Length field MUST be treated as padding and ignored on reception. If the packet is shorter than the Length field indicates, it MUST be silently discarded. The minimum length is 20 and maximum length is 4096.

Authenticator

The Authenticator field is sixteen (16) octets. The most significant octet is transmitted first. This value is used
to authenticate the reply from the RADIUS server.

Notification Authenticator

In User-Logoff-Notification packets, the Authenticator value is a 16 octet random number, called the Notification Authenticator. The value SHOULD be unpredictable and unique over the lifetime of a secret (the password shared between the client and the RADIUS server), since repetition of an authenticator value in conjunction with the same secret would permit an attacker to reply with a previously intercepted response. Since it is expected that the same secret MAY be used to authenticate with servers in disparate geographic regions, the Notification Authenticator field SHOULD exhibit global and temporal uniqueness.

The Authenticator value in an User-Logoff-Notification packet SHOULD also be unpredictable, lest an attacker trick a server into responding to a predicted future request, and then use the response to masquerade as that server to a future notification packet.

Although protocols such as RADIUS are incapable of protecting against theft of an authenticated session via realtime active wiretapping attacks, generation of unique unpredictable requests can protect against a wide range of active attacks against authentication.

Acknowledgement Authenticator

The value of the Authenticator field in the User-Logoff-Acknowledgement packet is called the Acknowledgement Authenticator, and contains a one-way MD5 hash calculated over a stream of octets consisting of: the RADIUS packet, beginning with the Code field, including the Identifier, the Length, the Notification Authenticator field from the User-Logoff-Notification packet, and the response Attributes, followed by the shared secret. That is,

\[
\text{Acknowledgement Auth} = \text{MD5(Code+ID+Length+NotificationAuth+Attributes+Secret)}
\]

where ‘+’ denotes concatenation.
Administrative Note

The secret shared between the client and the RADIUS server SHOULD be at least as large and unguessable as a well-chosen password. It is preferred that the secret be at least 16 octets. This is to ensure a sufficiently large range for the secret to provide protection against exhaustive search attacks. The secret MUST NOT be empty (length 0) since this would allow packets to be trivially forged.

A RADIUS server MUST use the source IP address of the RADIUS UDP packet to decide which shared secret to use, so that RADIUS requests can be proxied.

When using a forwarding proxy, the proxy must be able to alter the packet as it passes through in each direction - when the proxy forwards the request, the proxy MAY add a Proxy-State Attribute, and when the proxy forwards a response, it MUST remove its Proxy-State Attribute if it added one. Proxy-State is always added or removed after any other Proxy-States, but no other assumptions regarding its location within the list of attributes can be made. Since Access-Accept and Access-Reject replies are authenticated on the entire packet contents, the stripping of the Proxy-State attribute invalidates the signature in the packet - so the proxy has to re-sign it.

Further details of RADIUS proxy implementation are outside the scope of this document.

4. Packet Types

The RADIUS Packet type is determined by the Code field in the first octet of the Packet.

4.1 User-Logoff-Notification

Description

User-Logoff-Notification packets are sent to a RADIUS server as an indication that a previously authorized session has ended. A RADIUS client wishing to indicate the end of a user session MUST transmit a RADIUS packet with the Code field set to <MSG1> (User-Logoff-Notification).

Upon receipt of an User-Logoff-Notification packet from a
valid client, the server MUST reply using either a
User-Logoff-Acknowledgement message or a
Server-Error-Notification message [ERRMSG].

A User-Logoff-Notification message MUST contain either a
NAS-IP-Address Attribute [RFC2865] or a NAS-Identifier
Attribute [RFC2865] or both.

A User-Logoff-Notification message MUST contain a Session-Id
Attribute (see below) if one was returned from the server in
the Access-Accept message for the session; if no Session-Id
Attribute is included, the packet MUST contain a User-Name
Attribute and such additional Attributes as are necessary to
positively identify a given user session (e.g., Service-Type
[RFC2865], Calling-Station-Id [RFC2865], etc.).

To help avoid spoofing attacks, a User-Logoff-Notification
message SHOULD contain a Message-Authenticator Attribute
[RFC2869].

A summary of the User-Logoff-Notification packet format is
shown below. The fields are transmitted from left to right.

<table>
<thead>
<tr>
<th>Code</th>
<th>Identifier</th>
<th>Length</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Notification Authenticator</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Attributes ...</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Code

<MSG1> for User-Logoff-Notification

Identifier

The Identifier field MUST be changed whenever the content of
the Attributes field changes, and whenever a valid reply has
been received for a previous request. For retransmissions,
the Identifier MUST remain unchanged.

Zorn                   Expires November 11, 2004                [Page 7]
Notification Authenticator

The Notification Authenticator value MUST be changed each time a new Identifier is used.

Attributes

The Attribute field is variable in length, and contains the list of required Attributes, as well as any desired optional Attributes.

4.2 User-Logoff-Acknowledgement

Description

User-Logoff-Acknowledgement packets are sent by a RADIUS server as an acknowledgement that a previously authorized session has ended. A RADIUS server wishing to acknowledge the end of a user session MUST transmit a RADIUS packet with the Code field set to <MSG2> (User-Logoff-Acknowledgement).

No Attributes are required in a User-Logoff-Acknowledgement packet.

A summary of the User-Logoff-Acknowledgement packet format is shown below. The fields are transmitted from left to right.

```
0                   1                   2                   3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Code      |  Identifier   |            Length             |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
|                  Acknowledgement Authenticator                |
|                                                               |
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Attributes ... |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Code

<MSG2> for User-Logoff-Acknowledgement
Identifier

The Identifier field is a copy of the Identifier field of the User-Logoff-Notification packet which caused this User-Logoff-Acknowledgement packet to be created.

Acknowledgement Authenticator

The Acknowledgement Authenticator value is calculated from the User-Logoff-Notification packet, as described above.

Attributes

The Attribute field is variable in length, and contains any desired optional Attributes.

5. Attributes

5.1 Session-Id

Description

This attribute contains a unique identifier to make it possible for a RADIUS server to uniquely identify and track user sessions. In order to enable session tracking, this Attribute SHOULD be included in both the Access-Accept packet and the associated User-Logoff-Notification packet. The value of the Attribute in both messages MUST be the same.

The Identifier field of the Session-Id Attribute SHOULD contain UTF-8 encoded 10646 characters [RFC3629].

A summary of the Session-Id attribute format is shown below. The fields are transmitted from left to right.

```
0                   1                   2
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Type      |    Length     |    Identifier... |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Type

<A>TR> for Session-Id.
Length

>= 3

Identifier

The Identifier field SHOULD be a string of UTF-8 encoded 10646 characters [RFC3629].

6. IANA Considerations

The criteria to be used by the Internet Assigned Numbers Authority (IANA) for assignment of numbers within namespaces defined within this document are identical to those given in [RFC3575].

7. Security Considerations

If the User-Logoff-Notification packet is unauthenticated or if the shared secret is compromised, an attacker might be able to convince the server that user sessions had completed when they had not. If the server was limiting the number of simultaneous sessions, this could enable one or more users to exceed their session quota and possibly lead to service being denied to legitimate users.

8. References

8.1 Normative References


8.2 Informative References


Author's Address

Glen Zorn
Cisco Systems
2901 Third Avenue, Suite 600
Seattle, WA  98121
US

Phone: +1 425 344 8113
EMail: gwz@cisco.com
Intellectual Property Statement

The IETF takes no position regarding the validity or scope of any intellectual property or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; neither does it represent that it has made any effort to identify any such rights. Information on the IETF’s procedures with respect to rights in standards-track and standards-related documentation can be found in BCP-11. Copies of claims of rights made available for publication and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementors or users of this specification can be obtained from the IETF Secretariat.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights which may cover technology that may be required to practice this standard. Please address the information to the IETF Executive Director.

Full Copyright Statement

Copyright (C) The Internet Society (2004). All Rights Reserved.

This document and translations of it may be copied and furnished to others, and derivative works that comment on or otherwise explain it or assist in its implementation may be prepared, copied, published and distributed, in whole or in part, without restriction of any kind, provided that the above copyright notice and this paragraph are included on all such copies and derivative works. However, this document itself may not be modified in any way, such as by removing the copyright notice or references to the Internet Society or other Internet organizations, except as needed for the purpose of developing Internet standards in which case the procedures for copyrights defined in the Internet Standards process must be followed, or as required to translate it into languages other than English.

The limited permissions granted above are perpetual and will not be revoked by the Internet Society or its successors or assignees.

This document and the information contained herein is provided
on an "AS IS" basis and THE INTERNET SOCIETY AND THE INTERNET ENGINEERING TASK FORCE DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Acknowledgment

Funding for the RFC Editor function is currently provided by the Internet Society.