Internet Engineering Task Force
INTERNET-DRAFT
schulzrinne-sip-null.ps

SIP WG
Schulzrinne
Columbia U.

September 24, 2000
Expires: February 2000

SIP Authentication: The Null Authentication Scheme

Status of this Memo

Copyright Notice

Abstract

SIP servers may allow requests without authentication to proceed, possibly subjecting these unauthenticated requests to different handling. This memo describes the Null authentication method that simplifies the provision of such a service. This “authentication” scheme may also be useful for other protocols using the RFC 2617 framework.

1 Terminology

In this document, the key words “MUST”, “MUST NOT”, “REQUIRED”, “SHALL”, “SHALL NOT”, “SHOULD”, “SHOULD NOT”, “RECOMMENDED”, “MAY”, and “OPTIONAL” are to be interpreted as described in RFC 2119 [1] and indicate requirement levels for compliant SIP implementations.

2 Null Authentication Scheme

The “null” authentication scheme indicates that the client has no means of authenticating itself to the server. The “null” authentication scheme is considered useful for all protocols that employ RFC 2617-style authentication, such as SIP [2], RTSP [3] or HTTP [4].

The server will service the request only if no authentication is required. It SHOULD indicate to any server logic (such as sip-cgi [5] or CPL [6]) that the request has not been authenticated.

For Null, the framework in RFC 2617 [4] is utilized as follows:

```
challenge    =  ”Null”
credentials  =  ”Null”
```

There are no optional authentication parameters.

> SIP authentication differs somewhat from the requirements for web-page authentication. In some cases, recipients want to allow requests to reach the call processing logic or recipient even if they are not authenticated. However, such unauthenticated requests are then treated differently by the recipient. For example, a user might forward all unauthenticated SIP calls to a secretary or voicemail, or may disallow such calls during dinner hours. Given the possibly different treatment of authenticated and unauthenticated requests, it is useful to allow the server to challenge the client to obtain available credentials, yet make it possible for clients to submit requests that indicate that no credentials are available. If the client does not have credentials for the Request-URI, it then returns the Null credentials. The client could also provide the Null credentials immediately if it knows that it has no other credentials, avoiding an extra round-trip delay.
>
> The use of an empty WWW-Authenticate is not permitted by the HTTP/1.1 syntax, so an explicit authentication scheme name is needed.

Examples:

```
WWW-Authenticate: Null
Authorization: Null
```

A server MAY indicate that Null authentication is allowed in addition to “real” authentication methods, as in the following example:

```
WWW-Authenticate: Basic realm="Password, if you have it"
WWW-Authenticate: Null
```

3 Author’s Address

Henning Schulzrinne
Dept. of Computer Science
Columbia University
1214 Amsterdam Avenue
New York, NY 10027
USA
electronic mail: schulzrinne@cs.columbia.edu

References

[1] S. Bradner, “Key words for use in RFCs to indicate requirement levels,” Request for Comments 2119, Internet Engineering Task Force, Mar. 1997.

[2] M. Handley, H. Schulzrinne, E. Schooler, and J. Rosenberg, “SIP: session initiation protocol,” Request for Comments 2543, Internet Engineering Task Force, Mar. 1999.

[3] H. Schulzrinne, A. Rao, and R. Lanphier, “Real time streaming protocol (RTSP),” Request for Comments 2326, Internet Engineering Task Force, Apr. 1998.

[4] J. Franks, P. Hallam-Baker, J. Hostetler, S. Lawrence, P. Leach, A. Luotonen, and L. Stewart, “HTTP authentication: Basic and digest access authentication,” Request for Comments 2617, Internet Engineering Task Force, June 1999.

[5] J. Lennox, J. Rosenberg, and H. Schulzrinne, “Common gateway interface for SIP,” Internet Draft, Internet Engineering Task Force, May 1999. Work in progress.

[6] J. Lennox and H. Schulzrinne, “CPL: a language for user control of internet telephony services,” Internet Draft, Internet Engineering Task Force, Mar. 1999. Work in progress.

Full Copyright Statement