Network Working Group
Request for Comments: 3702
Category: Informational

J. Loughney
Nokia
G. Camarillo
Ericsson

February 2004

Authentication, Authorization, and Accounting Requirements for the Session Initiation Protocol (SIP)

Status of this Memo

Copyright Notice

Abstract

As Session Initiation Protocol (SIP) services are deployed on the Internet, there is a need for authentication, authorization, and accounting of SIP sessions. This document sets out the basic requirements for this work.

Table of Contents

1. Introduction

The AAA working group is chartered to work on authentication, authorization, and accounting solutions for the Internet. This work consists of a base protocol, applications, end-to-end security application, and a general architecture for providing these services [3]. The AAA working group has specified applicability of AAA-based solutions for a number of protocols (e.g., AAA requirements for Mobile IP [4]).

SIP is a signalling protocol for creating, modifying, and terminating different types of sessions, such as Internet phone calls, multimedia distribution, and multimedia conferences [1]. SIP sessions have needs for session authentication, authorization, and accounting (AAA).

In order to authenticate and authorize users, it is typically more convenient for SIP entities to communicate with an AAA sever than to attempt to store user credentials and profiles locally. SIP entities use the SIP-AAA interface to access the AAA server.

This document provides requirements for the interface between SIP entities and AAA servers. While accounting requirements are discussed, this document does not cover SIP charging or billing mechanisms.

One possible use of this document would be to create an AAA application for SIP. Any protocol meeting the requirements outlined by this document could be used. Possible candidates, among others, are Diameter [3] and XML-based protocols following the web-services model.

1.1. RADIUS

The main purpose of this document is to provide input to designers working on AAA applications using new protocols, such as Diameter and XML-based protocols. Nevertheless, a few limited RADIUS [5] extensions may meet some of the requirements in this document (for instance, some of the authentication requirements). We expect that while RADIUS with these limited extensions will meet particular functional requirements, it will not meet other important requirements. The following are some requirements that are not expected to be met by RADIUS:

1. Section 2.1.3: RADIUS does not support a discovery feature.

2. Section 2.1.7: RADIUS does not support reliable message delivery.

The following list contains the requirements that can be met by RADIUS or RADIUS extensions.

1. Section 2.1.2: Communication between domains does not scale well in RADIUS. As a result, inter-domain communications are typically handled using a proxy architecture [6].

2. Section 2.1.5: RADIUS clients would need to support Dynamic Authorization [7].

3. Section 2.1.9: RADIUS clients would need to rely on a lower-layer security protocol, such as IPSec, to perform mutual authentication.

4. Section 2.3.3: RADIUS clients would need to support Dynamic Authorization [7].

5. Section 2.3.4: RADIUS clients would need to support Dynamic Authorization [7].

1.2. Terminology and Acronyms

AAA: Authentication, Authorization, and Accounting

Accounting: The collection of resource consumption data for the purposes of capacity and trend analysis, cost allocation, auditing, and billing. Accounting management requires that resource consumption be measured, rated, assigned, and communicated between appropriate parties [8].

Accounting with credit control: The application checks the end user's account for coverage for the requested service event charge prior to execution of that service event.

Home AAA Server: Server where user with which the user maintains an account relationship.

SIP: Session Initiation Protocol

SIP proxies: SIP proxies are nodes which forward SIP requests and responses, as well as make policy decisions.

UAC: User Agent Client

UAS: User Agent Server

1.3. Requirements Language

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 BCP 14, RFC 2119 [2].

2. Requirements

In this section, we list the requirements. Protocol solutions are not required to satisfy requirements for services that they do not support. For example, a solution that provides authentication services but not accounting services does not need to fulfill the accounting requirements. It is expected that solutions will fulfill the general requirements, plus the requirements for the specific services they are providing.

Section 2.1 lists general requirements, Section 2.2 lists requirements related to authentication, Section 2.3 lists requirements related to authorization, and Section 2.4 lists requirements related to accounting.

2.1. Common Requirements

This section outlines general requirements on the SIP-AAA interface.

2.1.1. Communication within the Same Domain

The SIP-AAA interface MUST support communications between a SIP entity and an AAA server that belong to the same domain.

2.1.2. Communication between Different Domains

The SIP-AAA interface MUST support communications between a SIP entity in one domain and an AAA server in another domain. This MAY involve a proxy or a redirect server architecture between both entities.

2.1.3. Discovery

With the information contained in the SIP messages, the SIP-AAA interface SHOULD be able to deduce the particular AAA server that has to be queried.

2.1.4. Ability to Integrate Different Networks, Services and Users

The basic AAA architecture MUST be access independent. Service providers have to be able to provide AAA services for SIP, irrespective of access method or technology.

2.1.5. Updating SIP Server Entries

When required, the SIP-AAA interface MUST allow the AAA server to update the information that a SIP entity has about a user.

2.1.6. SIP Session Changes

The SIP-AAA interface MUST allow a SIP entity to inform the AAA server about changes in the SIP session that may affect the authorization, authentication, or accounting for that SIP session.

2.1.7. Reliable Transfer of Protocol Messages

The SIP-AAA interface SHOULD provide a reliable transfer of AAA protocol messages between the SIP entity and the AAA server.

2.1.8. Call Setup Times

AAA SHOULD NOT unduly burden call setup times where appropriate. It may be reasonable to support some delay during registration, but delay during on-going sessions (especially real-time) is problematic.

2.1.9. Security

The SIP-AAA interface is a potential target of an attack. An eavesdropper may attempt to obtain confidential data by sniffing messages. Additionally, an active attacker may attempt to modify, insert, or replay messages between the SIP entity and the AAA server. Attackers may also attempt to impersonate legitimate SIP entities or AAA servers.

To address these threats, the SIP-AAA interface MUST support confidentiality, data origin authentication, integrity, and replay protection. In addition to this, bi-directional authentication between the SIP entity and the AAA server MUST be supported as well.

2.2. Authentication Requirements

This section outlines requirements on the SIP-AAA interface related to authentication.

2.2.1. Authentication Based on SIP Requests

The home AAA server MUST be able to authenticate a user based on any SIP request, except CANCELs and ACKs for non-2xx final responses.

> CANCELs and ACKs for non-2xx final responses are hop-by-hop requests that can be generated by proxies that do not have the user's credentials.

2.2.2. Flexible Authentication of SIP Requests

The SIP-AAA interface MUST be flexible enough to accommodate a variety of authentication mechanisms used to authenticate SIP requests. In particular, the SIP-AAA interface MUST be able to accommodate all the authentication mechanisms mandated by the SIP specifications (e.g., Digest authentication).

2.3. Authorization Requirements

This section outlines requirements on the SIP-AAA interface related to authorization.

2.3.1. Ability to Authorize SIP Requests

The SIP-AAA interface MUST allow AAA servers to authorize any SIP request, except CANCELs and ACKs for non-2xx final responses.

> CANCELs and ACKs for non-2xx final responses are hop-by-hop requests that can be generated by proxies. SIP servers receiving a CANCEL or a ACK for a non-2xx final response do not challenge them, as they would do with an end-to-end request. Instead, they check at the transport or network layer that the entity sending the CANCEL or the ACK is the same as the one that generated the request being canceled or acked.

2.3.2. Information Transfer

The SIP-AAA interface MUST allow transferring a wide range or set of information to be used to make an authorization decision. In particular, the SIP-AAA interface MUST allow an AAA server that is making an authorization decision to deliver the user profile to the SIP entity. Such a user profile may provide further information about the authorization decision to the SIP entity.

For instance, a SIP proxy receives an INVITE from user A addressed to user B. The SIP proxy queries an AAA server and gets the following answer: user A is authorized to call user B, as long as the requests are routed through a particular SIP proxy server C. In this case, the SIP proxy needs to use SIP loose routing techniques to forward the INVITE so that it traverses SIP proxy C before reaching user B.

2.3.3. User De-authorization

The SIP-AAA interface MUST allow the AAA server to inform a SIP entity when a particular user is no longer authorized to perform a particular task, even if it is an ongoing task.

2.3.4. User Re-authorization

The SIP-AAA interface MUST allow the AAA server to inform a SIP entity that a particular authorization has been refreshed, and therefore, the user is still authorized to perform a particular task.

2.3.5. Support for Credit Control

The SIP-AAA interface MUST support credit control. That is, the AAA server has to be able to check the end user's account for coverage for the requested service event charge before authorizing execution of that service event. Note that this requirement is related to accounting as well.

Credit control is useful to implement prepaid services where all chargeable events related to a specific account are withheld from the end user when the credit of that account is exhausted or expired.

2.4. Accounting Requirements

This section outlines requirements on the SIP-AAA interface related to accounting. Accounting is more than simple charging. Accounting may be a simple list of services accessed, servers accessed, duration of session, etc. Charging for SIP sessions can be extremely complex and requires some additional study. It is not the intent of this section to focus on charging.

> The information available to be accounted is different at SIP proxies and at SIP UAs. When end-to-end encryption is used, proxies do not have access to some parts of the SIP messages, while UAs have access to the whole messages. In addition to this, UAs typically have information about the session itself (e.g., number of audio packets exchanged during an audio session). Therefore, even if the SIP-AAA interface provides a means to transfer a wide range of data, some SIP nodes may not have access to it. In order to design a network, it is important to analyze which SIP nodes will be able to generate the desired account records.

2.4.1. Separation of Accounting Information

AAA accounting messages MUST be able to provide granular information based on different parameters.

For example, it should be possible to separate "session duration" information from other information generated via additional services (e.g., 3-way calling). Separating accounting information makes it possible to provide accounting information to different parties based upon different aspects of the session.

2.4.2. Accounting Information Related to Session Progression

There MUST be support in the SIP-AAA interface for accounting transfers where the information contained in the accounting data has a direct bearing on the establishment, progression, and termination of a session (e.g., reception of a BYE request).

2.4.3. Accounting Information Not Related to Session Progression

There MUST be support in the SIP-AAA interface for accounting transfers where the information contained in the accounting data does NOT have a direct bearing on the establishment, progression, and termination of a session (e.g., an instant MESSAGE that is not related to any session).

2.4.4. Support for One-Time and Session-based Accounting Records

The SIP-AAA interface MUST allow SIP servers to provide relevant accounting information for billing and inter-network settlement purposes to the AAA servers. Both one-time event accounting records and session based (START, INTERIM, STOP records) accounting MUST be supported.

2.4.5. Support for Accounting on Different Media Components

The SIP-AAA interface MUST support accounting per media component (e.g., voice and video). That is, the SIP-AAA interface MUST be able to provide the AAA server with the types (e.g., voice and video) of the media streams of a given session.

Note, however, that some SIP entities do not have access to this information, which is typically carried in session descriptions. An example of a SIP entity with access to this information is a SIP UA (e.g., a gateway towards the PSTN).

The SIP-AAA interface MUST enable different parties to be charged per media component.

2.4.6. Configuration of Accounting Generation Parameters

The SIP-AAA interface MUST allow AAA servers to communicate parameters for accounting generation.

2.4.7. Support for Arbitrary Correlations

Some networks need to be able to relate accounting information to some aspect of the SIP messages involved. So, the SIP-AAA interface MUST allow the AAA server to correlate a particular AAA session with any aspect of the SIP messages. For example, an AAA server that receives accounting information about a SIP dialog may be interested in knowing the Call-ID of the SIP dialog.

3. Scenarios

This section outlines some possible scenarios for SIP and AAA interaction. These are purely illustrative examples and do not impose any requirements.

Figure 1 shows the typical call flow between a SIP proxy that communicates to an AAA server that performs authentication and authorization. All the examples are based on this flow.

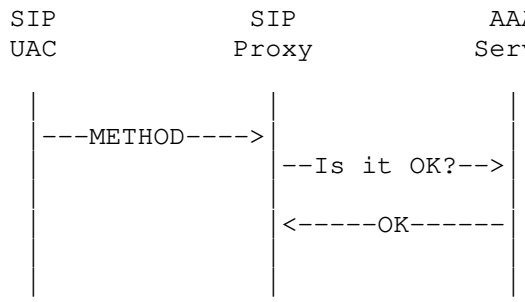

Figure 1: Call flow over the SIP-AAA interface

The SIP proxy receives a request with certain credentials. The SIP UAC that generated the request may have included the credentials after having been challenged by the proxy using a 407 (Proxy Authentication Required) response. The SIP proxy sends a request to the AAA server asking if it is OK to provide a particular service for this request. The service may be simply routing forward the request or may consist of a more complex service. The AAA server checks that the credentials are correct (authentication), and checks the user profile. The user profile indicates that it is OK to provide the service, and responds to the SIP proxy. The SIP proxy provides the service requested by the SIP UAC.

3.1. WLAN Roaming Using Third Party Service Providers

User A wants to establish a voice session over the Internet with user B. User A wants its SIP signalling to be routed through SIP proxy C, because it provides a call log service (i.e., SIP proxy C sends an email to user A once a month with the duration of all the calls made during the month).

```
                       SIP                AAA
     User A          Proxy C            Server           User B

        |                |                 |                |
        |----INVITE----->|                 |                |
        |                |                 |                |
        |<-----407-------|                 |                |
        |                |                 |                |
        |------ACK------>|                 |                |
        |                |                 |                |
        |----INVITE----->|                 |                |
        |                |---Is this OK?-->|                |
        |                |                 |                |
        |                |<------OK--------|                |
        |                |                 |                |
        |                |---------INVITE------------------>|
        |                |                 |                |
        |                |-Accounting msg->|                |
        |                |                 |                |
```

Figure 2: WLAN roaming user

User A accesses the Internet using a WLAN access outside his home domain. User A, user B, SIP proxy C, and the home AAA server of user A are all in different domains.

SIP proxy C challenges the initial INVITE from user A with a 407 (Proxy Authentication Required) response, and user A reissues the INVITE including his credentials. SIP proxy C consults user A's home AAA server, which confirms that the credentials belong to user A and that SIP proxy C can go ahead and provide its service for that call. SIP proxy C routes the INVITE forward towards user B and sends an accounting message to the AAA server, which will be used later to charge user A for the service provided by SIP proxy C.

3.2. Conditional Authorization

User A is not in his home domain, but he still uses SIP proxy C (which is in user's A home domain) as the outbound proxy for an INVITE. SIP proxy C consults the home AAA server, which indicates that requests from user A have to be routed through SIP proxy D. SIP proxy C uses SIP loose routing so that the INVITE traverses D before reaching its destination. SIP proxy D will provide a call log service for user A.

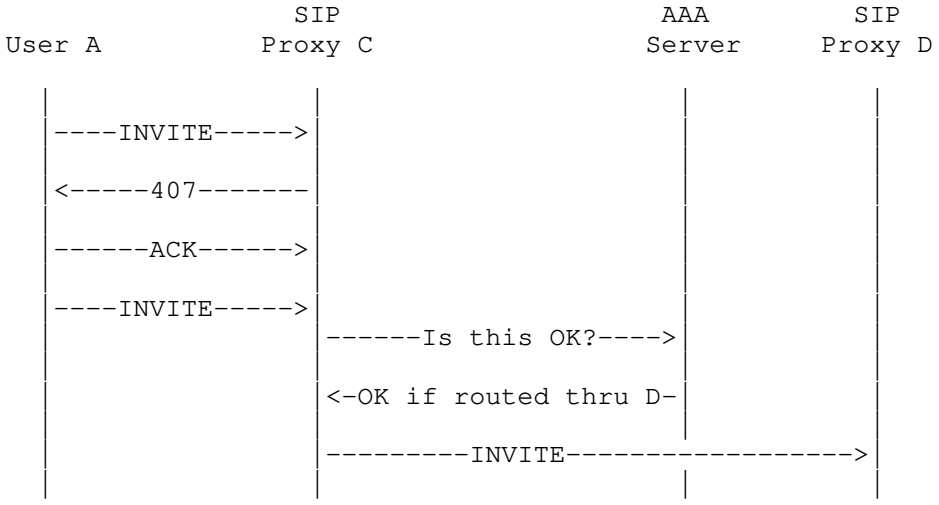

Figure 3: Conditional Authorization

4. Security Considerations

Security is a critical requirement of the SIP-AAA Interface. Section 2.1.9 describes the threats and security requirements. Sections 2.2 and 2.3 elaborate on the authentication and authorization requirements.

5. Acknowledgements

The authors would like to thank the participants of the SIP interim meeting, May 2002 for their comments. The authors would also thank Harri Hakala, Mary Barns, Pete McCann, Jari Arkko, Aki Niemi, Juha Heinanen, Henry Sinnreich, Allison Mankin, and Bernard Aboba for their comments.

The authors would like to thank the authors of the "AAA Requirements for IP Telephony/Multimedia" document, as it provided a basis for some of the information contained in this document.

6. References

6.1. Normative References

[1] Rosenberg, J., Schulzrinne, H., Camarillo, G., Johnston, A., Peterson, J., Sparks, R., Handley, M. and E. Schooler, "SIP: Session Initiation Protocol", RFC 3261, June 2002.

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

6.2. Informative References

[3] Calhoun, P., Loughney, J., Guttman, E., Zorn, G. and J. Arkko, "Diameter Base Protocol", RFC 3588, September 2003.

[4] Glass, S., Hiller, T., Jacobs, S. and C. Perkins, "Mobile IP Authentication, Authorization, and Accounting Requirements", RFC 2977, October 2000.

[5] Rigney, C., Willens, S., Rubens, A. and W. Simpson, "Remote Authentication Dial in User Service (RADIUS)", RFC 2865, June 2000.

[6] Aboba, B. and J. Vollbrecht, "Proxy Chaining and Policy Implementation in Roaming", RFC 2607, June 1999.

[7] Chiba, M., Dommety, G., Eklund, M., Mitton, D. and B. Aboba, "Dynamic Authorization Extensions to Remote Authentication Dial in User Service (RADIUS)", RFC 3576, July 2003.

[8] Aboba, B., Arkko, J. and D. Harrington, "Introduction to Accounting Management", RFC 2975, October 2000.

7. Authors' Addresses

John Loughney
Nokia
Itamerenkatu 11-13
00180 Helsinki
Finland

EMail: John.Loughney@nokia.com

Gonzalo Camarillo
Ericsson
Advanced Signalling Research Lab.
FIN-02420 Jorvas
Finland

EMail: Gonzalo.Camarillo@ericsson.com

8. Full Copyright Statement

Intellectual Property

Acknowledgement

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