Network Working Group
Request for Comments: 2977
Category: Informational

S. Glass
Sun Microsystems
T. Hiller
Lucent Technologies
S. Jacobs
GTE Laboratories
C. Perkins
Nokia Research Center
October 2000

Mobile IP Authentication, Authorization, and Accounting Requirements

Status of this Memo

Copyright Notice

Abstract

The Mobile IP and Authentication, Authorization, Accounting (AAA) working groups are currently looking at defining the requirements for Authentication, Authorization, and Accounting. This document contains the requirements which would have to be supported by a AAA service to aid in providing Mobile IP services.

1. Introduction

Clients obtain Internet services by negotiating a point of attachment to a "home domain", generally from an ISP, or other organization from which service requests are made, and fulfilled. With the increasing popularity of mobile devices, a need has been generated to allow users to attach to any domain convenient to their current location. In this way, a client needs access to resources being provided by an administrative domain different than their home domain (called a "foreign domain"). The need for service from a foreign domain requires, in many models, Authorization, which leads directly to Authentication, and of course Accounting (whence, "AAA"). There is some argument which of these leads to, or is derived from the others, but there is common agreement that the three AAA functions are closely interdependent.

An agent in a foreign domain, being called on to provide access to a resource by a mobile user, is likely to request or require the client to provide credentials which can be authenticated before access to resources is permitted. The resource may be as simple as a conduit to the Internet, or may be as complex as access to specific private resources within the foreign domain. Credentials can be exchanged in many different ways, all of which are beyond the scope of this document. Once authenticated, the mobile user may be authorized to access services within the foreign domain. An accounting of the actual resources may then be assembled.

Mobile IP is a technology that allows a network node ("mobile node") to migrate from its "home" network to other networks, either within the same administrative domain, or to other administrative domains. The possibility of movement between domains which require AAA services has created an immediate demand to design and specify AAA protocols. Once available, the AAA protocols and infrastructure will provide the economic incentive for a wide-ranging deployment of Mobile IP. This document will identify, describe, and discuss the functional and performance requirements that Mobile IP places on AAA protocols.

The formal description of Mobile IP can be found in [13,12,14,17].

In this document, we have attempted to exhibit requirements in a progressive fashion. After showing the basic AAA model for Mobile IP, we derive requirements as follows:

- requirements based on the general model
- requirements based on providing IP service for mobile nodes
- requirements derived from specific Mobile IP protocol needs

Then, we exhibit some related AAA models and describe requirements derived from the related models.

2. Terminology

This document frequently uses the following terms in addition to those defined in RFC 2002 [13]:

Accounting — The act of collecting information on resource usage for the purpose of trend analysis, auditing, billing, or cost allocation.

Administrative Domain
: An intranet, or a collection of networks, computers, and databases under a common administration. Computer entities operating in a common administration may be assumed to share administratively created security associations.

Attendant
: A node designed to provide the service interface between a client and the local domain.

Authentication
: The act of verifying a claimed identity, in the form of a pre-existing label from a mutually known name space, as the originator of a message (message authentication) or as the end-point of a channel (entity authentication).

Authorization
: The act of determining if a particular right, such as access to some resource, can be granted to the presenter of a particular credential.

Billing
: The act of preparing an invoice.

Broker
: An intermediary agent, trusted by two other AAA servers, able to obtain and provide security services from those AAA servers. For instance, a broker may obtain and provide authorizations, or assurances that credentials are valid.

Client
: A node wishing to obtain service from an attendant within an administrative domain.

Foreign Domain
: An administrative domain, visited by a Mobile IP client, and containing the AAA infrastructure needed to carry out the necessary operations enabling Mobile IP registrations. From the point of view of the foreign agent, the foreign domain is the local domain.

Inter-domain Accounting
: Inter-domain accounting is the collection of information on resource usage of an entity with an administrative domain, for use within another administrative domain. In inter-domain accounting, accounting packets and session records will typically cross administrative boundaries.

Intra-domain Accounting
: Intra-domain accounting is the collection of information on resource within an administrative domain, for use within that domain. In intra-domain accounting, accounting packets and session records typically do not cross administrative boundaries.

Local Domain
: An administrative domain containing the AAA infrastructure of immediate interest to a Mobile IP client when it is away from home.

Real-time Accounting
: Real-time accounting involves the processing of information on resource usage within a defined time window. Time constraints are typically imposed in order to limit financial risk.

Session record
: A session record represents a summary of the resource consumption of a user over the entire session. Accounting gateways creating the session record may do so by processing interim accounting events.

In this document, the key words "MAY", "MUST, "MUST NOT", "optional", "recommended", "SHOULD", and "SHOULD NOT", are to be interpreted as described in [4].

3. Basic Model

In this section, we attempt to capture the main features of a basic model for operation of AAA servers that seems to have good support within the Mobile IP working group. Within the Internet, a client belonging to one administrative domain (called the home domain) often needs to use resources provided by another administrative domain (called the foreign domain). An agent in the foreign domain that attends to the client's request (call the agent the "attendant") is likely to require that the client provide some credentials that can be authenticated before access to the resources is permitted. These credentials may be something the foreign domain understands, but in most cases they are assigned by, and understood only by the home domain, and may be used for setting up secure channels with the mobile node.

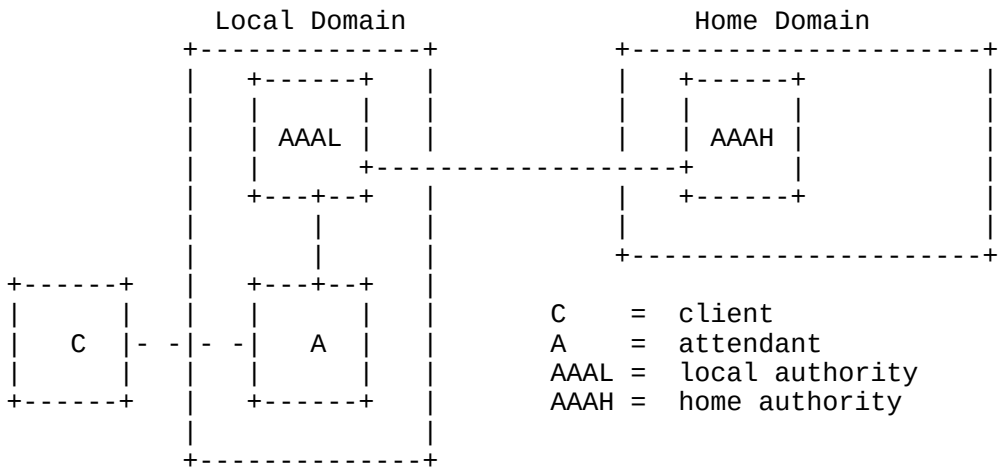

Figure 1: AAA Servers in Home and Local Domains

The attendant often does not have direct access to the data needed to complete the transaction. Instead, the attendant is expected to consult an authority (typically in the same foreign domain) in order to request proof that the client has acceptable credentials. Since the attendant and the local authority are part of the same administrative domain, they are expected to have established, or be able to establish for the necessary lifetime, a secure channel for the purposes of exchanging sensitive (access) information, and keeping it private from (at least) the visiting mobile node.

The local authority (AAAL) itself may not have enough information stored locally to carry out the verification for the credentials of the client. In contrast to the attendant, however, the AAAL is expected to be configured with enough information to negotiate the verification of client credentials with external authorities. The local and the external authorities should be configured with sufficient security relationships and access controls so that they, possibly without the need for any other AAA agents, can negotiate the authorization that may enable the client to have access to any/all requested resources. In many typical cases, the authorization depends only upon secure authentication of the client's credentials.

Once the authorization has been obtained by the local authority, and the authority has notified the attendant about the successful negotiation, the attendant can provide the requested resources to the client.

DOCKET ALARM

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS
Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS
Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS
Sync your system to PACER to automate legal marketing.