Quality of Service Authentication, Authorization and Accounting

Tseno Tsenov[1], Hannes Tschofenig[1]

Siemens AG, Otto-Hahn-Ring 6, Munich 81739, Germany
hannes.tschofenig@siemens.com, tseno.tsenov@mytum.de

Abstract. Proper authorization is essential for a QoS signaling protocol. The policy control of future QoS signaling solutions is expected to make use of existing AAA infrastructure for computing the authorization decision. In this paper, we point to two approaches for QoS authorization (based on COPS and Diameter) and present possible extensions and directions for future work.

1 Introduction

To meet the Quality of Service (QoS) requirement for applications such as Voice-over-IP in a heavily loaded network, packets belonging to real-time application must be identified and segregated from other traffic to ensure that the bandwidth, delay, and loss rate requirements are met. This requires explicit reservation techniques. In addition to the verification of resource availability, authentication and authorization of the requests are required, especially in an environment where the endpoints are not trusted. A variety of QoS protocols exist, including RSVP [1] and the NSIS QoS NSLP [3]. In this paper, we present a short overview of the framework, proposed solutions and future work.

2 Framework

Policy control for QoS signaling is conceptually organized as illustrated in Fig. 1. Network elements through which application flows need to pass, a cloud of Policy/AAA servers and an Authorizing entity/PDP are shown. A resource request sent by the end host is intercepted at a router along the path. This router will offload the authorization decision to the AAA backend infrastructure. The request will, for example, be routed to the home network, where the home AAA server will return a decision. Not all of the routers are policy-aware since policy enforcement is likely to be concentrated on the borders of an administrative domain.

2.1 COPS usage for RSVP

RFC 2749 [2] is a part of a framework for policy-based control over admission control decisions for QoS signaling using RSVP. The Common Open Policy Service (COPS) protocol is used to exchange policy information between a Policy

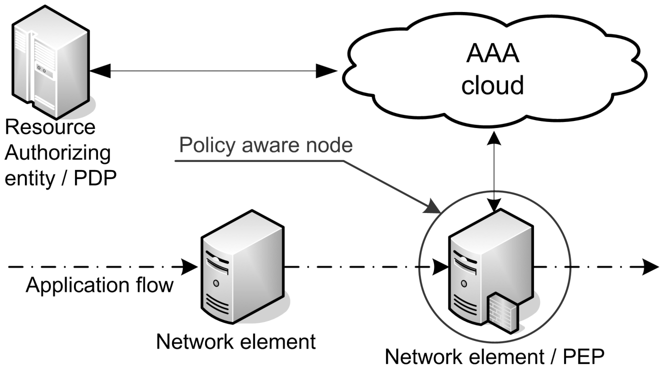

Fig. 1. Policy Control Architecture

Decision Point (PDP) and a set of RSVP routers (Policy Enforcement Points, PEPs). At the event of incoming RSVP request, the entire RSVP message is encapsulated in COPS REQ message and sent to the PDP. The PDP is assumed to implement the same RSVP functional specification as the PEP and share the RSVP state. A decision is taken at the PDP, based on the policy data object and other objects from the RSVP message.

2.2 NSIS QoS NSLP and Diameter QoS Application

The Diameter QoS application, in contrast to COPS, might be used by QoS NSLP capable nodes along the path of a given application flow to contact an authorizing entity/application server, located somewhere in the network, providing an AAA service of the reservation request [5]. This allows for a wide variety of deployment models. Extending the Diameter protocol includes the use of new mandatory AVPs and Command-Codes that are required to enable QoS authorization.

A generalized QoS parameter format is used by the Diameter QoS application (taken from the NSIS QSPEC template [6]) that allows the Diameter QoS application to be combined with virtually all QoS signaling protocols. An authorizing server would use the QoS parameters in addition to an authorization token included in the QoS-Authorization Request message to make a decision. After a positive authorization decision, the router starts an accounting session. Session termination may be initiated by both sides. Possible causes might be a NSIS tear down message, loss of bearer report, insufficient credits or session termination at the application layer.

3 Extended QoS Authorization

With the support for one-pass authentication methods (including authorization tokens/Kerberos tickets [8]) not all deployment scenarios can be addressed adequately. Existing QoS protocols currently lack the support for a generic three party authorization model that includes support for:

- Challenge-Response-based Authentication and Key Agreement (AKA),
- EAP-based Authentication and Key Agreement (AKA)

These two approaches show the tradeoff between the flexible choice of AKA protocols and complexity. EAP provides a high degree of flexibility with a certain amount of inefficiency and complexity (see [5]). Both approaches provide better security properties than a token-based approach [7] due to the active involvement of the end host and better integration into existing network architectures regarding key distribution.

Beyond adding new payloads, it is essential to evaluate the security implications of the three party exchange as part of the keying framework.

4 Summary and outlook

Unlike the approach followed with RSVP, where the entire RSVP message is encapsulated into a COPS message, the Diameter QoS application includes only the relevant fields from a QoS NSLP message, avoiding the overhead of transmitting irrelevant objects for the AAA infrastructure. Together with a generic QoS format, the Diameter QoS application is less dependent on a particular QoS signaling protocol or a particular QoS model. Diameter plays an important role for accounting and charging in an inter-domain environment and is therefore ideally suited for QoS authorization. Many of the functions provided by Diameter are lacking in COPS. A number of security related open issues have been identified (see [4] and [5]).

References

1. Braden, R., Zhang, L., Berson, S., Herzog, S., Jamin, S.: Resource ReSerVation Protocol (RSVP) – Version 1 Functional Specification. RFC 2205 (Proposed Standard) (1997) Updated by RFCs 2750, 3936.
2. Herzog, S.: COPS Usage for RSVP. RFC 2749 (2000)
3. Van den Bosch, S., Karagiannis, G., McDonald, A., : NSLP for Quality-of-Service signaling. Internet draft (draft-ietf-nsis-qos-nslp-06), work in progress (2005)
4. Alfano, F., McCann, P., Tschofenig, H.: Diameter Quality of Service Application. Internet draft (draft-alfano-aaa-qosprot-02), work in progress (2005)
5. Tschofenig, H., Kross, J.: Extended QoS Authorization for the QoS NSLP. Internet draft (draft-tschofenig-nsis-qos-ext-authz-00), work in progress (2004)
6. Ash, J., Bader, A., Kappler, C.: QoS-NSLP QSpec Template. Internet draft (draft-ietf-nsis-qspec-03), work in progress (2005)
7. Hamer, L., Gage, B., Kosinski B., Shieh H.: Session Authorization Policy Element. RFC 3520 (2003)
8. Baker, F., Lindell, B., Talwar M.: RSVP Cryptographic Authentication. RFC 2747 (2000)