An Access Control System for Multimedia Content Distribution

Manuel Sánchez[1], Gabriel López[1], Óscar Cánovas[2], Juan A. Sánchez[1], and Antonio F. Gómez-Skarmeta[1]

[1] Department of Information Engineering and Communications
[2] Department of Computer Engineering
University of Murcia, Spain
{msc, gabilm, jlaguna, skarmeta}@dif.um.es,
ocanovas@ditec.um.es

Abstract. Multimedia content distribution has appeared as a new growth market offered by network providers, defining resource access infrastructures able to support both wired and wireless accesses. Although these infrastructures have been widely studied in the last years, the main aim of those works has been focused more on the distribution process than on a suitable security infrastructure to protect that content. Therefore, the study of security systems able to offer authentication, authorization and other security-related requirements for those kinds of scenarios is still an open research field. In this paper, we propose a new scheme which takes advantage of a previously existing underlying authorization infrastructure among the involved organizations, the NAS-SAML system, to build a multimedia content distribution with an advanced and extensible authorization mechanism. The target scenario is the one proposed by the VIDIOS project, which defines an architecture for multimedia transmissions across error prone networks such as Internet backbones and mobile access networks.

1 Introduction

Wireless and wired broadband accesses are a strategic growth market covered by almost all European network providers. European Internet Service Providers (ISP) identified multimedia content distribution as a potential means to create significant revenue above pure infrastructure business. In fact, video streaming is regarded as a short term emerging service with several different opportunities, ranging from personal video conferencing to video on demand.

One of the main concerns of a multimedia distribution system is to protect the distribution process against malicious users. First, it is necessary to ensure that only users which have paid the fees can access to the system. Second, the system must ensure that the protected content is only obtained by those users with the appropriate access level, that is, only by authorized users. Finally, the confidentiality and integrity of the multimedia streaming must be protected from passive and active attacks.

It is worth noting that in these scenarios, where multimedia contents are transported from providers to customers through open data networks, it is possible to find inter-domain scenarios, for example when the domain providing the multimedia content and the costumer's ISP domain are different. Moreover, users can access to the content

A.S. Atzeni and A. Lioy (Eds.): EuroPKI 2006, LNCS 4043, pp. 169–183, 2006.

provider from different ISPs. This involves an explicit agreement among the involved domains in order to exchange the information needed to perform access control functions, as well as the QoS enforcement.

Although access control is a key feature in content distribution, this is not an exclusive topic of this field. Traditionally, organizations have protected critical resources, for example the communication network. In fact, the AAA architecture [15] was designed to solve this last problem, using different mechanisms to identify end users, such as login/password or identity certificates. Therefore, one of the most common access control mechanisms used by network providers is the one based on the AAA architecture.

In this paper, we present an access control architecture developed for the VIDIOS project [10], an international consortium composed by eight institutions (T-Systems International, FH Mannheim, Quix, Satec, Scopus, Telefonica, University of Goettingen and University of Murcia). Among the main aims of this project is the design and validation of an architecture for delivering multimedia content, especially MPEG-4 encoded video, over a Multi Protocol Label Switching (MPLS) backbone. Due to the similarities we can find regarding other existing access control architectures, it would be desirable to reuse most of the ideas and contributions included in the existing proposals to define the access control architecture for VIDIOS. In fact, a successfully tested system such as NAS-SAML [20] will be used as the starting point of the authentication, authorization and QoS enforcement scenarios. As we will see, NAS-SAML makes use of XML-based standards to manage the authentication and authorization data and to express the access control policies in an extensible and distributed way.

The rest of this paper is structured as follows. Section 2 defines the VIDIOS project. Then, Section 3 establishes the main requirements of the access control architecture once we have analyzed the main goals of VIDIOS. Section 4 introduces the NAS-SAML system, which will be used as the starting point to define the access control architecture. Next, Section 5 presents the main elements of that architecture and Section 6 details the way the authentication, authorization and QoS enforcement is finally performed. Section 7 shows some details about the implementation. Section 8 describes the related work that informed our research. Finally, we conclude the paper with our remarks and future directions.

2 VIDIOS

VIDIOS designs and validates an architecture which delivers end-to-end Quality of Service for multimedia transmissions across error prone networks such as Internet backbones and mobile access networks. MPEG-4 Advanced Video Coding, combined with robust and scalable coding techniques are applied by VIDIOS for robust transport over a MPLS backbone. The MPLS backbone further protects the application stream by QoS based on already implemented standards.

Figure 1 shows a basic overview of the VIDIOS functionality. This image shows the content provider (CP) where the user is registered and two different ISP domains. Users can access to the service through any of the ISPs, as long as the ISP has an agreement with the CP. This agreement must specify the QoS that the ISP has to provide to its customers, which is directly related to the access level the user has subscribed with