Chapter VII

Multimedia Security and Digital Rights Management Technology

Eduardo Fernandez-Medina, Universidad de Castilla-La Mancha, Spain

Sabrina De Capitani di Vimercati, Università di Milano, Italy

Ernesto Damiani, Università di Milano, Italy

Mario Piattini, Universidad de Castilla-La Mancha, Spain

Pierangela Samarati, Università di Milano, Italy

ABSTRACT

Multimedia content delivery applications are becoming widespread thanks to increasingly cheaper access to high bandwidth networks. Also, the pervasiveness of XML as a data interchange format has given origin to a number of standard formats for multimedia, such as SMIL for multimedia presentations, SVG for vector graphics, VoiceXML for dialog, and MPEG-21 and MPEG-7 for video. Innovative programming paradigms (such as the one of web services) rely on the availability of XML-based markup and metadata in the multimedia flow in order to customize and add value to multimedia content distributed via the Net. In such a context, a number of
security issues around multimedia data management need to be addressed. First of all, it is important to identify the parties allowed to use the multimedia resources, the rights available to the parties, and the terms and conditions under which those rights may be executed: this is fulfilled by the Digital Rights Management (DRM) technology. Secondly, a new generation of security and privacy models and languages is needed, capable of expressing complex filtering conditions on a wide range of properties of multimedia data. In this chapter, we analyze the general problem of multimedia security. We summarize the most important XML-based formats for representing multimedia data, and we present languages for expressing access control policies. Finally, we introduce the most important concepts of the DRM technology.

### INTRODUCTION

Multimedia information (such as free text, audio, video, images, and animations) is of paramount importance for human-computer interaction in a number of application fields, such as entertainment, distance learning, pay-per-view/listen business, and collaboration among others. Multimedia security problems are very similar to traditional security problems, but there are some important aspects that make more complex the solutions: traditional multimedia documents usually are monolithic, without a clearly defined internal structure, they are conceived to be discretionally distributed, they are easy to clone, easy to modify, to remove, to manipulate, and so on. Recently, the importance of complementing binary multimedia data with metadata in the form of XML tagging has been fully realized. XML-based standards formats for multimedia, such as SVG (SVG, 2001), SMIL (SMIL, 2001), and VoiceXML (VoiceXML, 2002) make the internal structure of multimedia flows available to consumer applications and devices. These languages describe the internal properties of the multimedia documents, making possible to refer to structural or semantic components, such as keywords, and graphical/audio/audiovisual properties.

The wealth of semantics- and structure-related information carried by these new XML-based multimedia formats suggests that the time has come to develop novel approaches for controlling access and fruition of multimedia content. In particular, a number of security issues around multimedia data management need to be addressed. Figure 1 illustrates a Multimedia Security Taxonomy according to which multimedia security encompass techniques to determine who can use multimedia content and at what conditions (controlled fruition); to prevent multimedia content from being illegally copied (prevention); and to protect multimedia content while it is being transmitted or stored (privacy). In the following, we describe these problems in more detail.
Designing a Secure Cloud Architecture: The SeCA Model

[www.igi-global.com/article/designing-secure-cloud-architecture/64344?camid=4v1a](http://www.igi-global.com/article/designing-secure-cloud-architecture/64344?camid=4v1a)