32
How to Protect Multimedia Applications

Eckhard Koch
Fraunhofer Institute for Computer Graphics
Wilhelminenstr.7, 64283 Darmstadt, Germany,
phone: +49-6151-155147; fax: +49-6151-155444
e-mail: ekoch@igd.fhg.de

Abstract

New kinds of application and the convolution of different media types require a specific approach to fulfill the arising security demands. In principle, the security of a multimedia system can be supplied on the level of the network, the application and the data. This paper concentrates on the security of the application and data level, decribes various requirements and outlines possible solutions to protect multimedia applications.

Keywords

multimedia applications and data, security platform, application programming interfaces, use control, copyright protection

1 INTRODUCTION

The most significant advancements in cryptography were made about 20 years ago by developing the public key cryptography. On the one hand, the key management, especially the distribution of secret keys, was simplified, and, one the other hand, it was made possible to set digital signatures necessary for electronic business transactions. The main application areas were confined to performing authentication as well as to ensuring confidence, integrity, and non-repudiation via simple point-to-point communication.

In the field of multimedia communication and information services the development has been enforced during the last years. New kinds of applications and services have been developed like groupwork applications (CSCW), broadcasting services (Pay-TV, video on demand, interactive TV, hypermedia information services (WWW)). On the other side, the information and communication technology of today - in contrast to the former, mainly text-oriented computer communication - features a combined use and a merging of all sorts of media types.

When developing these new multimedia applications and constructing the system architectures the solution of basic technical problems was in the foreground and thus the integration of security functionality was mostly neglected.

J. L. Encarnação et al. (eds.), *Mobile Communications*

Now these systems and applications are leaving the research community and enter mainstream commercial applications, the lack of appropriate security techniques is becoming more and more an obstacle to the real-world applicability of multimedia systems and applications.

This paper is mainly describing the requirements which come forth when security solutions are added to the existing applications and the possible solutions. Furthermore, the specific problems and solutions of the protection of multimedia data are presented.

2 REQUIREMENTS

In principle, security of a system can be supplied on the level of

- the network and the respective protocols
- the application and
- the data

These levels, however, do not exclude but complement each other. Several security provisions may be done on the network and respective protocol level. Some security requirements, however, cannot be met on this level, like the deliberate setting of a digital signature, the authentication of the actual user, the specific cryptographic treatment of images, video etc. or the protection of the intellectual property of multimedia data (copyright protection).

For these application-, data-, and user-specific requirements expedient and adequate solutions can only be found on the application and data levels.

2.1 Application Level

In order to avoid different security solutions for every specific application and application protocol and to remain flexible towards the use of new applications and services the use of a generic security platform seems reasonable for the integration of security on the application level. This security platform should meet the following requirements (Gehrke and Koch, 1995):

- independence from application,
- independence from security technology,
- independence from communication,
- compatibilty and interoperability,
- media-specific operations.

The last issue offers the possibity to differentiate between media types and to apply specific operations to protect multimedia data.

2.2 Data Level

The main objective in introducing this level of protection is to have some means of control and protection of multimedia data after secure transmission and delivery by any kind of application. This is mainly caused by the needs of any information and content provider who hesitates to offer valuable data without any control on the use and any technical means to protect their intellectual property.

From the technical point of view two requirements can be identified. Firstly, after the secure delivery of digital information to an authorized user it would be neccessary to control the operations the user is allowed to perform. They can cover a wide range of allowed actions, e.g. the right to view, display, manipulate, or copy the multimedia data. Secondly, the multimedia data have to be marked or labeled in some way that allows to identify the ownership, the rights etc. to the data after distribution. This information (mark) has to be embedded into the multimedia data, in a way that the mark is perceptually invisible, unremovable, unalterable and furthermore survives processing which does not seriously reduce the quality of the multimedia data.

3 SECURING MULTIMEDIA APPLICATIONS

To fulfill the various requirements outlined above a security plattform has to offer an application-independent Application Programming Interface (API). This could be the Generic Security Service API (GSS-API, RFC 1508,1509) or a similar one. Using such kind of API allows to plug the security platform in different kinds of application. Furthermore, due to the nature of this API the security of the system is independent of the transport layer and specific communication protocols, because the communication is handled by the application itself.

The requirement to distinguish between different kind of multimedia data can be fulfilled by introducing the concept of filters. The filter has to be integrated into the application and passes the different media to the security platform in order to process them seperately.

To be independent of the security technology means to be able to use any security algorithm and method, hard-, soft- or firmware. This can be reached by the use of a technology-independent API which has to be implemented between the application-independent API and the crypto modules.

One of the critical issues - not only in the field of security - is the interoperability between different security platforms, methods and concepts. Interoperability can be obtained to a certain degree by implementing various quasi-standard security modules and data formats below the technology-independent API. Surely, it has to be indicated by each communication partner which technology he supports. But describing this with a formal security policy allows to negogiate a common configuration of the security platform on sender and receiver side.

The intense demand in such flexible security architecture has led to a first implementation of a platform for secure multimedia applications (Krannig, 1995). This security platform is based on an object-oriented approach which facilitates the compliance with the requirements.

4 PROTECTING MULTIMEDIA DATA

Control of the usage of multimedia data on receiver side is difficult to introduce and to perform from the legal, social and technical point of view. A specific rendering device (filter) has to be installed on user side

- to control which rights (e.g. print, display, copy) to which piece of information the user has and
- to account, monitor and trace the usage

On service provider side the information has to be prepared for controlled distribution, which means the multimedia data have to be marked, encrypted, signed and encapsulated. On the user side only the specific device can handle and use the prepared and protected information. This device can be implemented in software and/or hardware and can be integrated as plug-in module in the user's application (e.g. a WWW browser).

Once in possession (e.g. by means of authorized copying) of the information there is no further protection possible, except for marking or labeling the multimedia data. A digital (water-)mark can discourage illicit copying and dissemination of (proprietary) information by making misuse traceable and by providing evidence of misbehavior. By embedding information about the ownership, rights, etc. a proof of ownership is possible, by embedding information about the authorized recipient the distribution path can be tracked.

Meanwhile various watermarking schemes are under development (Koch and Zhao, 1995, Macq and Quisquater, 1995). A key issue is to mark the data in a secure and robust way.

5 CONCLUSION

Today security is not a stand-alone solution. Security always has to be linked to the corresponding applications and the data which have to be protected. Therefore security on application and data level will play an increasing role in securing already existing and future multimedia applications.

6 REFERENCES

Gehrke, M. and Koch, E. (1995) A security platform for future telecommunication applications and services. In: *Proc. of the 6th Joint European Networking Conference* (JENC6), Tel Aviv.

Koch, E. and Zhao J. (1995) Towards robust and hidden image copyright labeling. In: *Proc. of IEEE Workshop on Nonlinear Signal and Image Processing*, Neos Marmaras.

Krannig, A. (1996) PLASMA - Platform for secure multimedia applications. In *Communications and Multimedia Security*, IFIP Joint Working Conference TC-6 and TC-11, Essen, to be published.

Macq, B. and Quisquater, J.J. (1995) Cryptology for digital TV broadcasting. In: Proc. of the IEEE, vol. 83, no. 6.

RFC 1508, 1509 (1993), Generic Security Service API.

7 BIOGRAPHY

Eckhard Koch studied physics and received his doctor degree in 1993. After this he joined the Fraunhofer Institute for Computer Graphics as head of the department 'Security Technology for Graphics and Communication Systems'. He is partner in several European projects working on access control for broadcasting services and copyright protection. Besides this, he leads several industrial and national projects in his department. These projects deal with the integration of security services in information and communication systems, the development of cryptographic methods for multimedia data. Special attention is given to data compression, face and voice recognition, copyright protection and digital watermarking.