A Privacy-Friendly Electronic Payment Model: Balancing Copyright and Privacy Protection Requirements

[1]V. C. Zorkadis, [2]D. A. Karras, and [1]E. S. Siougle
[1]Data Protection Authority, Omirou 8, 10564 Athens, Greece,
[2]Hellenic Aerospace Industry, Rodu 2, Ano Iliupolis, Athens 16342, Greece,
GREECE

Abstract: The electronic distribution of digital works leads to the collection and processing of huge amounts of personal data, and copyright management information. However, international treaties, EU Directives and National Laws contain provisions which protect these data, i.e. there are statutory obligations related to the protection of privacy, copyright management and electronic transactions. The enforcement of the legal framework requires the employment of appropriate security and organizational measures. To address these problems, we propose a privacy-friendly electronic payment model, which aims at balancing contradicting copyright and privacy protection-related requirements. With our model, electronic consumers can anonymously order and pay digital works, while the media distributors involved in the transaction and the copyright owners are protected against intellectual property rights violations. The entities involved in the transactions, range from creator and copyright holder to media distributor, the monitoring and the privacy service provider and the bank gateway.

Key words: Copyright Protection; Electronic Payment Systems; Privacy Protection; Privacy-Enhancing Technologies; Network Privacy and Anonymity; Privacy-Friendly Network-Based Transactions.

1. Introduction

Significant application developments in the last decade, based on the broad deployment of open - oriented information and communication infrastructures, allow the extensive electronic distribution of digital works. The main business actors involved in these transactions are the digital work (creator and) producer, the retailer, and the digital content consumer. Besides the security threats encountered, there are further risks related to copyright protection and privacy, which may derive from the involved actors due to their different needs. Digital work producers are interested in that neither the retailers nor the consumers make and distribute any illicit copies. Retailers are interested in that consumers do not make any illicit copies from the digital contents acquired and that they would not be unjustifiably accused of having reproduced illegal replicas. Finally, consumers may be essentially concerned with their privacy protection, i.e. that their personal data are not collected and misused for profile creation and direct marketing.

To cope with the mentioned problems, copyright management information must be incorporated in digital works and appropriate security and privacy protection mechanisms in electronic payment systems. Various areas of law offer partial protection, such as unfair competition law, trademark law and liability and criminal law. Specific national laws based on the WIPO Treaties and the EU Directives may provide better legal protection. According to the Directive 2001/29/EC, of the European Parliament and of the Council, on the harmonization of certain aspects of copyright and related rights in the information society, there is legal protection against removal or manipulation of copyright management information.

In particular, according to the European Directive, Member States shall provide adequate legal protection against the circumvention of any effective technological measures. Also, Ìember States shall provide for adequate legal protection against any person knowingly performing without authority any of the following acts: (a) the removal or alteration of any electronic rights-management information; (b) the distribution, importation for distribution, broadcasting, communication or making available to the public of works or other subject-matter protected under this Directive from which electronic rights-management information has been removed or altered without authority.

On the other hand, international legal instruments such as European Directives 95/46/EC and 97/66/EC, the Council of Europe's Convention of the Protection of individuals with regard to Automatic Processing of Personal Data, and the OECD's Guidelines Governing the Protection of Privacy and Trans-border Flows of Personal Data [3,4] provide privacy protection. According to the European Directives, the main principles, which comprise the basis of the legal framework related to data protection, are the following [13]:

- Personal data should be gathered by fair and lawful means and the amount of personal data collected should be adequate, relevant and not excessive in relation to the purposes for which they are processed.
- Personal data should be collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes, and should be accurate and up to date. Inaccurate or incomplete personal data should be erased or rectified, and personal data should be preserved in a form, which permits identification of the data subjects for no longer than is required for the purpose for which those data are stored.
- Security measures should be taken to protect personal data from unintended or unauthorized disclosure, destruction or modification.

To achieve the fulfillment of these contradicting requirements, appropriate payment models have to be applied, characterized by minimal personal data used, while assuring copyright protection.

The paper is structured as follows. The next section shortly presents system actors and the security, privacy and copyright protection requirements. The third section is devoted to a short description of our proposed payment model. In the fourth section, we analyze security aspects of this model. Finally, we conclude the paper.

2. System Analysis and Security, Privacy, Copyright Protection Requirements

The components (actors) involved in our model are shown in Fig. 1, reflecting business models such as IMPRIMATUR [11] and entities needed for security, privacy and copyright protection. The user or acquirer may be a business, an administration or individual. In this paper, we focus on individuals as users, since they have privacy–related requirements, though businesses may also, in some cases, pose similar objectives.

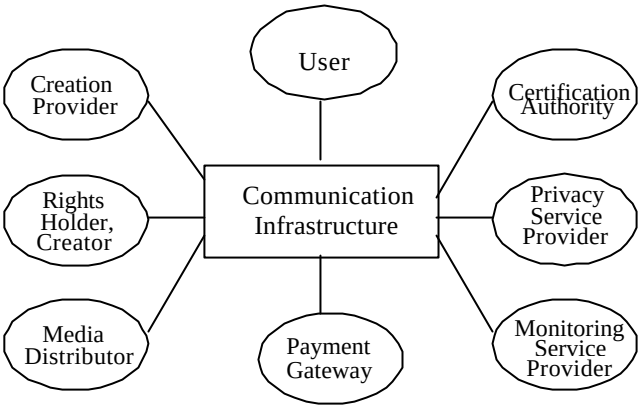

Figure 1: Components of the Privacy-Enhancing Payment Model

A user may register with a certification authority or with a privacy service provider, or directly with a media distributor if he is not interested in privacy protection. Furthermore, he may obtain digital money by e-banks or payment gateways. We assume regarding users, that they are mainly interested in acquiring digital goods, while preserving their privacy and without taking risks being unjustifiably accused of making illegal use of them.

Rights holders or creators aim at exploiting their digital works, by making them available to a wider audience, in most cases with the support of creation providers and media distributors. Their requirements range from technical control over the distribution of digital products to resolution of legal issues such as taxation and liability. In our model, it is assumed that rights holders cooperate with creation providers, though they would take on the role of them, but at a cost of managing rights and payment mechanisms. Outsourcing the management of rights and payment mechanisms would be a solution to this problem.

Small and medium sized creation providers are expected to rely on media distributors to get their products to digital markets, as opposed to large companies which are expected to have also the role of media distributor. Creation providers agree with rights holders to commercialize their creations according to specific terms, which comprise the CP - RH agreement. On the other hand, they also have to join a contract with media distributors.

Media distributors cooperate with both creation providers and users, providing interfaces for browsing product information, delivery and payment. They may also provide information management and brokerage functions. Media distributors may add new value on digital works, as creation providers also do, creating composite digital objects, from multiple sources (creation providers), thus requiring automatic right clearance, simple procedures to obtain licenses and multiparty payment mechanisms.

Monitoring service providers constitute functional entities, responsible with monitoring the legal usage of licensed digital goods, according to rights terms agreed upon acquisition. They may be functional part of a media distributor. However, more likely, they may be part or constitute a separate third party, trusted by all involved entities, namely rights holders, creation providers, media distributors and users.

Payment gateways are e-banks involved on-line or off-line in payment procedures and issuing digital money. Finally, certification authorities and privacy service providers are trusted third parties enabling the use of public key based cryptographic applications and anonymous or pseudonymous authentication procedures. Certification authorities and privacy service providers may be functional units of the same physical entity or separate entities.

To cope with security, privacy and copyright related threats, the following mechanisms should be applied: authentication, confidentiality, integrity, authorization / access control, non-repudiation, privacy protection and copyright protection. Prior to data communication or electronic transactions, the peer entities must mutually authenticate themselves. To prevent unauthorized data disclosure, data encryption is applied. Symmetric cipher systems may be used. Also, content integrity or authenticity must be provided and the application of appropriate authorization and access control procedures by all actors is assumed. To implement integrity or authenticity mechanisms one-way hash functions and digital signature schemes may be used.

Furthermore, the provision of non-repudiation mechanisms is required, so that neither a customer (user) nor a media distributor can repudiate an order or the receipt of a payment. Again, for the implementation of non-repudiation mechanisms, digital signature schemes may be used. Though data encryption may provide some protection against privacy violations, it cannot be adequate, since traffic data such as sender's and receiver's identities or source and destination addresses, time of the communication and information volume exchanged are still exposed to interception. Privacy protection may be achieved with support by privacy service providers and by means of techniques based on anonymity or pseudonyms. Finally, copyright protection mechanisms must be applied, so that copyright violations of digital works can be detected. They should base on resistant watermarking or fingerprinting techniques, which allow the secure insertion of copyright management information in multimedia content or digital works.

3. Privacy-Friendly Distribution - Payment Model

We distinguish two phases in our model, the preparation and the purchase-payment phase. During the preparation phase, users address themselves to certification authorities to obtain public key certificates, to privacy service providers to obtain pseudonymous public key certificates, to electronic banks to obtain revocable anonymous digital money and to media distributors to register in case they receive subscription – based services. Also, creation providers, media distributors, monitoring service providers (MSP) and other model actors obtain their

public key certificates. Furthermore, creation providers apply to a Publication Issuing Certificate Authority (PICA) for a publication authorization license (PAL) [14], consisting of a publication authorization number (PAN), a publication date, specific information as submitted by creation providers and rights holders and a content digest. The specific information may reflect agreement terms between creators or rights holders and creation providers and may be formed by a trusted third party, such as a monitoring service provider. PICA signs the publication authorization license with its signature computation key. Next, creation providers usually advertise their digital products and media distributors may apply for a publication-selling license (PSL), which should be signed either by the content provider or the trusted third party involved in this process. PSLs may contain, besides PAL, related information to their agreement, such as time validity of PSL, digests of concrete terms, etc.

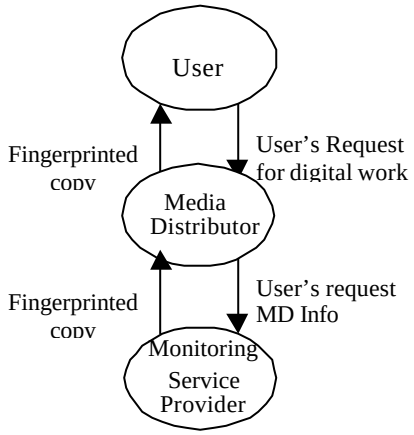

Figure 2: Messages exchanged between the model actors

Now, it is possible for a user to pseudonymously order a digital work by a media distributor and pseudonymously pay for it, while ensuring copyright protection, if the following procedures are applied. A user or customer may directly contact a media distributor to order a digital work by giving its PAL, indicating the payment manner chosen and using her/his pseudonymous key to sign this purchase request message (PRM). Upon receipt of the PRM, the media distributor forwards to monitoring service provider info related to this order. The monitoring service provider forms the watermark information consisting of PAL, PSL, and PRM id, including the pseudonymous public key certificate of the user and inserts it into a copy of the ordered digital work. This watermarked copy is sent to media distributor, which forwards it to the user, who ordered it along with a payment request. The monitoring service provider sends also a message to creation providers containing the PSL and PRM id informing them of the order. After having received the ordered watermarked digital work, the user can pay by means of revocable anonymous e- money. Facing the media distributor the possibility the user not to pay after receiving the digital work may lock the usage of the content copy till user's payment. Alternatively, the payment may come along with the order, so that the risk for the media distributor not to obtain the payment after having sent to user the ordered digital work is eliminated.

4. Security Analysis

To analyze the security of the proposed model we may consider various scenario attacks expected to be encountered in this electronic distribution environment. Customers may try to repudiate the order or the receipt of an ordered digital work and media distributors may repudiate the receipt of payment. Also, customers may collude to remove copyright management information, media distributors may try to illegally reproduce and distribute copyrighted digital works possibly causing troubles for customers, media distributors may collude with customers trying to defraud content providers and right holders, etc. The first scenario – attack can be coped with, since the pseudonymous public keys are revocable, i.e. privacy service providers can reveal the real identities of the users only in cases legal disputes. Against the second scenario-attack, the user should lock the e-money contained in a payment message by means of a secret key and require by the media distributor to acknowledge this message. Then, the user can unlock the e-money allowing media distributors to use it. Protection against other threats is offered through the selection of appropriate

watermarking techniques, that are robust against collusion attacks and the involvement of monitoring service providers in the distribution process.

5. Summary/Conclusion

We presented a generic privacy and copyright protection model, which is proposed for anonymous transactions while maintaining favorable conditions which enable copyright protection. In our model, the entities involved in the transactions are the user, the privacy service provider, the media distributors, the content provider, the monitoring service provider, the payment service provider (gateway) and the network gateways. The users obtain tokens (pseudonyms) from privacy service providers and anonymous digital money from payment gateways to use in their transactions with media distributors. The user tokens are contained in the fingerprints, formed by the monitoring service provider and inserted along with further information in the digital works, to enable user identification in the case of illegal reproduction of the digital work. The anonymous payment may be supported on-line by the payment gateway, which notifies the related entities involved in the transaction, so that intellectual rights can be protected and piracy can be discouraged. Alternatively, the payment gateway may be involved off-line in the payment process, in which case the transaction is completed without prior share of the payment according to the union agreement between the involved entities.

Our model fulfils the contradicting demands of copyright owners and digital work consumers, since the former require copyright protection and the latter their privacy protection, satisfying thus the need for balancing them.

References:

[1] I. J. Cox, J. Kilian, T. Leighton, and T. Shamoon, "A Secure, Robust, Watermark for Multimedia", *Workshop in Information Hiding, vol. 1174 LNCS*, Springer Verlag, pp. 185-206, 1996.

[2] I. J. Cox, J. Kilian, T. Leighton, and T. Shamoon, "Secure Spread Spectrum Watermarking for Multimedia", *IEEE Transactions on Image Processing*, vol. 6, no. 12, pp. 1673-1687, 1997.

[3] I. Pitas, "A Method for Signature Casting on Digital Images", *Proc. of Int. Conf. on Image Processing*, vol. III, pp. 215-218, 1996.

[4] F. A. P. Petitcolas and Ross J. Anderson, "Evaluation of copyright marking systmes", *Proc. of IEEE Multimedia Systems '99*, vol. 1, pp. 574-579, 1999.

[5] F. A. P. Petitcolas, Ross J. Anderson and M. Kuhn, "*Attacks on copyright marking systems*", Workshop in Information Hiding, vol. 1525 LNCS, Springer Verlag, pp. 218-238, 1998.

[6] IMPRIMATUR (IMP/I4062/A), "Watermarking Technology for Copyright Protection: General Requirements and Interoperability", pp. 1-14, www.imprimatur.net.

[7] F. Mintzer, G. W. Braudaway and M. M. Young, "Effective and ineffective digital watermarks", *Proc. of Int. Conf. on Image Processing*, vol. III, pp. 9-12, 1996.

[8] ISO/IEC 9796, Information technology – Security techniques – Digital signature schemes giving message recovery, (1991), and 1997.

[9] ISO/IEC 14888, Information technology – Security techniques – Digital signature schemes with appendix, 1998.

[10] W. J. Caeli, E. P. Dawson, S. A. Rea, "PKI, Elliptic Curve Cryptography, and Digital Signatures", *J. Computers & Security*, 18 (1999), pp. 47-66.

[11] IMPRIMATUR (IMP/3-0021), "Business Modeling", pp. 1-18, www.imprimatur.net.

[12] IMPRIMATUR (IMP/3-0021), "Protection of Copyright Management Information", 1998, pp. 1-42

[13] V. Zorkadis, E. Siougle, 'Information Security and Privacy Audit Modeling', *Proc. of the 5th World Multiconference on Circuits, Systems, Communications and Computers*, Crete, July 2001

[14] Yu-Lu Huang, Shiuh-Pyng Shieh, Fu-Shen Ho, "A Generic Electronic Payment Model Supporting Multiple Merchant Transactions", *J. Computers & Security*, Vol. 19, No. 5, p. 453-465, 2000.