Privacy-Preserving Digital Rights Management

Antoni Roig
UAB Institute of Law and Technology (IDT), Universitat Autònoma de Barcelona, Spain

Abstract. Digital Rights Management (DRM) is a technology that provides content protection by enforcing the use of digital content according to granted rights. DRM can be privacy-invasive due to many reasons. The solution is not easy: there are economic and legitimate reasons for distributors and network operators to collect data about users and their activities, such as traffic modelling for infrastructure planning or statistical sampling. Furthermore, traditional PET – such as encryption, anonymity and pseudonymity– cannot solve all the privacy problems raised by DRM, even if they can help. Privacy and security considerations should be included in the design of DRM from the beginning, and they should not be considered as a property that can be added on. PET is considered as technology for privacy protection, in different fields. However, PET solutions are not the only ones to be considered useful to complement DRM systems. The contrary is also true: DRM systems are adapted as technical platforms for privacy. In short, there is a deep change in PET related to the web 2.0, and it is also true for P2DRM: transparency and other new techniques are preferred, or at least added, to anonymity, authentication and other traditional protections.

Keywords: Privacy Enhancing Technology (PET), Digital Rights Managements (DRM), Privacy-Preserving Digital Rights Management (P2DRM), Privacy-Friendly Design.

1. DRM has the potential for threatening privacy

Digital Rights Management (DRM) is a technology that provides content protection by enforcing the use of digital content according to granted rights (Conrado et al. 2004). A DRM system normally includes content protection, rights creation and enforcement, identification of users and usage of content monitoring:

- Security and integrity features of computer operating systems, for instance, file-access privileges.
- Rights-management languages that determine whether requested uses should be allowed.
- Encryption
- Digital signatures provide assured provenance of digital content and non repudiation of transactions.

- Fingerprinting and other “marking” technology so as to facilitate copy tracking, distribution or usage. User tracking or network control of users’ computers are potentially destructive for user privacy. Data collection by distributors and network operators can be a real problem for user’s privacy.

- Thus, DRM can be privacy-invasive due to many reasons (Feigenbaum et al. 2002):

- DRM does not support anonymous or unlinkability, so it is quite different from buying a CD paying cash.
- DRM content acquisition is also privacy-invasive. A distributor may use complete DRM metadata with digital content. Each file downloaded by a user from the distributor’s web would include both the content and the metadata with the “rights” that the user has acquired. So the user could only access the content as specified by the metadata. And the rights’ metadata are minable as user information.
- The device uploaded can also be privacy-invasive. The download could be oriented to a specific device with a serial number. The device is then the user’s information that can be collected and mined. The upload of the device, due to malfunctioning or purchase of a new one, also offers the possibility of tracking user’s information.
- Another DRM privacy problem is the usage track. The downloaded content of the user can also be mined and collected. The potential tracking of a concrete user’s information includes all its listening, viewing and reading.
- Finally, there are economic reasons for collecting user’s data. For instance, DRM data networks should provide usage tracking for efficient management and artists’ compensation, but should not provide user tracking. Personal Identifying Information (PII) such as names, addresses and telephones should be preserved; for example, using anonymous payment.

2. Traditional Privacy Enhancing Technologies (PET) cannot solve all problems

2.1. LIMITS

The solution is not easy. There are economic and legitimate reasons for distributors and network operators to collect data about users and their activities; for example, traffic modelling for infrastructure planning or statistical sampling. Furthermore, traditional PET, like encryption, anonymity and pseudonymity cannot solve all the privacy problems raised by DRM, even if they may help (Feigenbaum et al., 2002).

2.2. CRYPTOGRAPHY

While cryptography is useful for the Trusted Computing Base (TCB), it is considered inadequate for commercial content distribution (Feigenbaum *et al.*, 2002). Cryptography needs to define exactly whether there is legitimate use of data or not and what the single relationship between two identified persons or institutions is. Another difficulty with cryptography is that public-key cryptography is slow, so if privacy in DRM uses this possibility, it will reduce considerably the rate of simultaneous connections. On the other hand, DRM will not generally accept cryptographic e-cash but it will rather continue with credit cards. As a result, vendors will have the possibility of learning how much is paying someone.

2.3. AUTHENTICATION

Traditional authentication can also be criticized. The management of users' identity should be based on recognition rather than authentication (Seigneur, 2009). As Seigneur says, in an authentication process there is:

- Enrolment: generally involves an administrator or human intervention.
- Triggering: someone clicks on a web link to a resource that requires authentication to be downloaded.
- Detective work: the main task is to verify that the entity's claimed identity is correct.
- Action: the identification is subsequently used in some ways.
- On the other hand, recognition consists of:
- Triggering (passive and active sense): the recognising user can trigger itself.
- Detective work: recognising the user.
- Upper-level action (optional): the outcome of the recognition is subsequently used in some ways.

The recognition process is an example of a more general replacement for authentication that does not necessarily bind an identity to the recognised identity. On the contrary, authentication is a recognition process that binds a real-world identity to the virtual identity. The possibility of recognising a user, analysing some of its attributes, is sufficient to establish trust based on past experience. One way of preserving both privacy and trust is using pseudonyms. Nevertheless, traffic analysis, data triangulation and data-mining can also associate a pseudonym with the real user. That is the reason why it is important that multiple pseudonyms are provided.

Technical solutions, such as a trust transfer, can be adopted then to avoid the misuse of multiple pseudonyms (Seigneur, 2009). Another example is the EU-funded FP6 project PRIME (Privacy and Identity Management for Europe), whose approach uses “private credentials”. This private credentials enable proving one’s authorization (e.g., to be over 18 years old) without identifying the individual. They are derived from certificates issued on different pseudonyms of the same person, and they are neither linkable to each other nor to the issuance interaction. Only in the case of misuse, the user’s anonymity can be revoked (Hansen, 2008).

2.4. FUTURE TRENDS

Consumers are largely unable to differentiate between privacy options: “Best practices” for privacy engineering have not yet been standardized. Even if businesses decide to offer privacy, like Earthlink and its “totally anonymous Internet” or Zero-Knowledge Freedom network with its pseudonymity, this consumer inability to differentiate motivates companies not to invest in expensive technological options (Feigenbaum *et al.*, 2002).

Indeed, the desire for preserving user’s privacy in DRM may not be enough motivation to force an infrastructural change. Some interim steps are needed in today’s infrastructure. Even if consumers seem more and more concerned about privacy, they do not use at the moment significant privacy-preserving tools. New PET and privacy design principles are needed for this purpose, at every stage of DRM-system design, development and deployment, as can be seen later. Let’s begin with design and then see implementations of Privacy-Preserving Digital Rights Management (P2DRM).

3. Privacy-friendly Design (or Engineering) for DRM

3.1. PRINCIPLES

Privacy and security considerations should be included in the design of DRM from the beginning and they should not be considered as a property that can be added on. In fact, integrating privacy tools in legacy systems poses many problems (Feigenbaum *et al.*, 2002). First, dual operation due to compatibility of two designs is easy to attack. Second, legacy systems might expect more information than the information provided by the privacy device. Third, legacy systems might expect different performance than the one offered by the privacy protocol. Finally, there may be a congestive collapse of networking in the legacy system.

Some guidelines of privacy protection, the so-called Fair Information Principles (FIP) or general principles of the E. U. Data Protection Directive, may be useful as practical privacy engineering. Below there is a list with general goals which are not concrete technological options:

- Collection limitation
- Data accuracy
- Purpose disclosure
- Use limits
- Security
- Openness
- Participation
- Organizational accountability

3.1.1. *Collection Limitation*

A system should work with *minimal data exchanges* and PII should not be included by default. A first design decision is to analyze the need for information and to determine how the information flow can be minimized. Most of the system applications will only need pseudonyms instead of PII. Proxies can help a collection-limitation approach. Indeed, a trusted third party that provides some seal of approval may be preferable than an audit that happens after data collection.

3.1.2. *Data Accuracy*

If PII is necessary, then it should be erased after its immediate need has been fulfilled.

3.1.3. *Purpose Disclosure*

Notices should be easily understandable.

3.1.4. *Openness*

The idea is to combine notice and auditability. A company will not want to be exposed by violating its advertised privacy policy.

3.1.5. *Low cost solutions*

The advantage of such general goals or FIPs is that it allows us to consider low-cost solutions for privacy-preserving electronic commerce technologies. Technological solutions are not always necessary or useful for each problem. Some of these low-cost solutions might be (Feigenbaum *et al.*, 2002):

- Privacy enhancement should be built directly into the DRM technology that powers consumer applications. No additional steps to protect their privacy should be necessary.
- The business costs of introducing privacy enhancement into DRM should be low.
- The consumer costs, including “user experience”, of using privacy-enhanced DRM should also be low.

3.2. TECHNIQUES

On the other hand, some authors consider that it is time to not only include privacy goals, but also concrete privacy preserving techniques to help engineering designers from the beginning. For instance, *PriS* is an engineering method which incorporates privacy requirements early in the system development process (Kalloniatis et al., 2008). Privacy requirements are considered as organisational goals that need to be satisfied. *PriS* provides a description of the effect of privacy requirements on business processes, and it allows the identification of the best privacy-preserving system architecture.

PriS conceptual model is based on the Enterprise Knowledge Development (EKD) framework (Kavakli and Loucopoulos, 1999), which develops organisational knowledge. It models the organisational goals of the enterprise, the processes and the software systems that support the above mentioned processes. As a result, a connection is established between system purpose and system structure. Privacy requirements are a special type of goal, privacy goals, which constraint the causal transformation of organisational goals into processes. One relevant aspect of *PriS* is that it indicates the concrete technique available to the designer for a goal, once adapted to respect a privacy requirement. So, it’s useful during the design, and it helps to bridge the gap between design and implementation.

4. New PET for DRM (P2DRM)

4.1. LICENCES

PET is usually considered technology for privacy protection in different fields. Nonetheless, Korba and Kenny have observed that the interests a service user has in dealing with sensitive data are similar to those of providers of copyrighted digital contents (Korba, 2002). Thus, not only are PET solutions considered useful to complement DRM systems, but the contrary is also true: DRM systems are adapted as technical platforms for privacy.

For instance, this happens for data protection. One of the aims of data protection regulation is control over ones' data. Furthermore, data protection is known in Germany as the so-called self-determination of personal data right. Users need more control over their transmitted data, or during the use of a service (Hohl, 2007). If we consider sensitive personal data, it is sent in a protected way to the service provider. This encrypted data has a license attached to it when communicated to the service providers. The license limits the use of this personal data. It uses then classical anonymization techniques and the concepts of data minimality and data obfuscation (Hohl, Zugenmaier, 2007).

Privacy-preserving DRM system, or P2DRM, should also allow a user to interact with the system in an anonymous/pseudonymous way while buying and consuming digital content. On the other hand, this has to be done in a way that content is going to be used according to issued licenses and cannot be illegally copied (Conrado *et al.*, 2004).

We have already said that some authors consider cryptography inadequate for DRM. For others P2DRM can be based on cryptography. The idea is that a possible disclosure of the association between the user who transfers and the user who receives a given license is a privacy concern. This can be avoided with revocation lists and generic (or anonymous) licenses issued by the content provider (Claudine Conrado *et al.*, 2004). The licenses are anonymous in the sense that they do not include any identifier of the user who bought or exchanged his old license for the anonymous license. However, they include a unique identifier to prevent that an anonymous license is copied and redeemed multiple times. In the case of licenses in an authorized domain, the solution proposed is private creation and functioning, preventing the content provider from learning which domain members composes a domain (Koster, 2006). A domain manager device, trusted by the content provider, is introduced to solve privacy problems within the domain.

Personalized restrictions in specific domains are also a proposed solution (Petkovic, 2006). One possibility for a user to protect his interest and privacy is to apply some access control on licenses or content that he obtains from the content provider. However, access control only offers a limited functionality. Therefore a solution is a DRM system that allows the user to set further restrictions on the licenses obtained from the content provider. The proposed method is based on a specific form of a delegation license, called star-license, and an activation mechanism. The star-licenses allow adding further restricting rights-expressions by indicating who may define further restrictions and activate the license (Petkovic *et al*, 2006.).

4.2. DISTRIBUTED DRM

Another PETDRM or P2DRM solution can be a distributed DRM (Abie, 2004). The design of this system is based on trusted systems (Sadeghi, 2007). In the core of the system, a Privacy Enforcement Module (PEM) allows the privacy officer to define and update privacy policy. On the basis of this policy, it will allow or disallow actions. When a request is made for access to certain privacy sensitive elements or operations on an information object, the request is sent to the PEM. The PEM then decides whether the operation is to be permitted or not (Abie *et al*, 2004).

4.3. MOBILE DRM

Mobile DRM needs also new technical solutions. Even if it is not strictly a PET, the guaranty of non-repudiation is perhaps not only useful for DRM, but also for P2DRM. Non-repudiation is in charge of ensuring that no party can deny having participated in a transaction (Onieva, 2007). So having evidences of malicious activities by any of the peers may help. This service has not been included so far in DRM specifications due to practical issues and the type of content distributed. Non-repudiation can also protect privacy, and more precisely "sensitive information" such as financial statement, medical records, and contracts available in digital form. If we want to securely store this sensitive information, share it or distribute it within and between organizations, non-repudiation is an adequate technical solution. A non-repudiation protocol must generate cryptographic evidence to support eventual dispute resolution. A *trusted third party* (TTP) usually helps entities to accomplish their goals. One interesting aspect of the protocol of non-repudiation proposed by Onieva *et al.* (2007) is that anonymity could be preserved. In that sense, neither the content provider nor the user needs any knowledge (i.e., digital certificates) about each other in order to reach a successful protocol end.

4.4. DRM FOR PRIVACY INFORMATION RETRIEVAL (PIR)

Another P2DRM to consider is DRM for PIR (Asonov, 2004). PIR provides such an execution of user queries over a database of digital goods that no information about user queries is revealed, even to the server that actually accesses the digital goods. All a provider can do is to count the number of queries issued by a single user, and to charge it on a pay-per-query basis. In a strict version of PIR, DRM cannot be managed. Asonov's (2004) idea is to eliminate this conflict between DRM and user privacy relaxing the privacy constraint of PIR. He considers the possibility of revealing some information about user queries in order to be able to perform the distribution of interests of DRM. Indeed, users should be able to deny any claims about their queries. This repudiation capacity transforms PIR in Repudiative Information Retrieval (RIR). Furthermore, the precision of the DRM system depends on the robustness of the repudiation provided.

4.5. LOCATION BASED SERVICES

Location Based Services (LBS), like PDA, will also generate a wide range of DRM-privacy issues. Gunter *et al.* describe an architecture based on Personal Digital Rights Management (PDRM), which uses DRM concepts as a foundation for the specification and negotiation of privacy rights (Gunter, 2005). Their prototype, *AdLoc*, manages advertising interrupts on PDA based on location determined by WiFi sightings in accordance with contracts written in the DRM language XrML. PDRM uses the same DRM mechanisms to enable individuals to license their private data. Indeed, PDRM can specify that a private telephone number can only be used once for a specific purpose. The prototype approach, as stated before, is based on the use of the XrML digital rights language with negotiated privacy rights derived from specific sectors.

4.6. PLATFORMS

Multilateral-secure platforms can also offer P2DRM solutions. Sadeghi *et al.* describe a multilateral-secure DRM platform that can preserve some aspects of privacy (Sadeghi, 2005). The platform can be realized based on existing open platform technologies and trusted computing hardware like a Trusted Platform Module (TPM). An interesting aspect is that discrimination of open-source software due to TPM can be solved by a property-based attestation described by the authors.

4.7. SITDRM

Sheppard *et al.* (2006) have implemented a privacy protection system (SITDRM Enterprise) based on the Intellectual Property Management and Protection (IPMP) components of the MPEG-21 multimedia framework (Sheppard, 2006). This seems better than using the P3P policy language for expressing the privacy preferences of data subjects. P3P is adequate to inform data subjects of the global privacy practices of Internet service providers. However, users have to specify their preferences regarding a particular item of data in DRM. Nevertheless, P3P is used more recently in a complementary way with SITDRM to communicate enterprise privacy policies to consumers, and enable them to easily construct data licenses

(Salim, 2007). SITDRM required the design of an extension to the MPEG Rights Expression Language (MPEG-REL) to cater for privacy applications, and the development of software that allowed individuals' information and privacy preferences to be securely collected, stored and interpreted. The possibility of a future grand unified DRM system seems technically feasible, but the authors doubt about the utility of such a non-specific tool.

5. Conclusions

In 2002, Feigenbaum *et al.*, were convinced that a *practical methodology for privacy engineering* was necessary, involving procedures for the analysis of privacy-relevant aspects of a system. Nevertheless, they advise that developing such a methodology even for the problem of DRM systems would be quite challenging. Has the situation changed from 2002?

Every new PET seems to have difficulties to be implemented after its theoretical formulation. This is also true with respect to DRM. But there is a new element that can make the difference in this case: DRM systems are also adapted in a way to protect privacy. So PET for DRM and DRM adapted to privacy are converging in P2DRM. This can be useful for designing and implementing P2DRM from the PET perspective, or from the DRM one. So PET and DRM specialists should consider the new field an opportunity for respecting both DRM and privacy goals.

We have seen that authentication can adapt to a non-identification version, more flexible and less dangerous for privacy. Nonetheless, there is a deep change in PET related to the web 2.0 which is also true for P2DRM: transparency and other new techniques are preferred to anonymity, authentication and other traditional protections. Old PET are still useful, but they do not give enough guaranty to new privacy threatens. The value of transparency tools depends on how precise and understandable the information is. Standardization could help humans to understand and machines to interpret the information made transparent. Another challenge is that a transparency process can be also privacy-invasive. So data minimization with minimal disclosure of personal information is usually more effective than relying on "notice and choice" (Hansen, 2008). Context and purpose limitation attach to the identifiable data is also a new PET tool useful with web 2.0, the participatory Web (Weiss, 2008).

References

Abie H., Spilling P., and Bent F. (2004), *A distributed digital rights management model for secure information-distribution systems*, International Journal of Information and Security num. 3, pp. 113–128.

Asonov D. (2004), *Querying Databases Privately*, LNCS 3128, Springer, Heidelberg, Berlin, pp. 77–97.

Conrado C., Petkovic M., and Jonker W. (2004), in Jonker W. and Petkovic M. (Eds.),” SDM 2004”, Springer, Heidelberg, Berlin, pp. 83–99.

Feigenbaum J., Freedman M.J., Sander T., and Shostack A.(2002), in Sander T. (Ed.), “DRM 2001”, Springer, Heildelberg, Berlin, pp. 76–105.

Gunter C.A., May M.J., and Stubblebine S.G. (2005), *A Formal Privacy System and Its Application to Location Based Services*, in D. Martin and A. Serjantov (Eds.), “PET 2004”, Springer, Berlin, New York, pp. 256–282.

Hansen, M., (2008), in Simone Fischer-Hübner, Penny Duquenoy, Albin Zuccato, Leonardo Martucci (Eds), *The Future of Identity in the Information Society*, IFIP International Federation for Information Processing, Volume 262, Springer, Boston, pp. 199–220.

Hohl, A. and Zugenmaier, A. (2007), in Venter, H., Eloff, M., Labuschagne, L., Eloff, J., and Von Solms, R. (Eds.), *New Approaches for Security, Privacy and Trust in Complex Environments*, IFIP International Federation for Information Processing, Volume 232, Springer, Boston, pp. 449-456.

Kalloniatis C., Kavakli E. and Gritzalis S. (2008), *Addressing Privacy Requirements in System Design: the PriS Method*, Requirements Engineering 13, pp. 241–255.

Kavakli V. (1999), *Enterprise knowledge management and conceptual modelling*, LNCS, vol. 1565, Springer, Berlin, pp 123–143.

Kavakli, V. and Loucopoulos, P. (1999), *Modelling of Organisational Change Using the EKD Framework*, Communications of the Association for Information Systems (CAIS), Vol 2.

Korba, L., and Kenny, S. (2003), *Towards Meeting the Privacy Challenge: Adapting DRM*, ACM Workshop on Digital Rights Management, Springer, Berlin.

Onieva J.A., López J., Román R., Zhou J., and Gritzalis S. (2007), *Integration of non-repudiation services in mobile DRM scenarios*, Telecommun Syst, 35, pp. 161–176.

Sadeghi A.-R., Wolf M., Stüble C., Asokan N., and Ekberg J.-E. (2007), *Enabling Fairer Digital Rights Management with Trusted Computing*, in Garay J. et al. (Eds.), ISC 2007, LNCS 4779, pp. 53–70.

Sadeghi A.-R. and Stüble C. (2005), *Towards Multilateral-Secure DRM Platforms*, in Deng, R. H. et al. (Eds.), ISPEC 2005, LNCS 3439, pp. 326–337.

Salim F., Sheppard N.P., and Safavi-Naini R. (2007), *Enforcing P3P Policies Using a Digital Rights Management System*, in Borisov N. and Golle P. (Eds.), PET 2007, LNCS 4776, pp. 200–217.

Seigneur J.M. (2009), *Social Trust of Virtual Identities,* in Golbeck J. (ed.), Computing with Social Trust, Human-Computer Interaction Series, Springer-Verlag, London.

Sheppard N.P. and Safavi-Naini R. (2006), *Protecting Privacy with the MPEG-21 IPMP Framework*, in Danezis G. and Golle P. (Eds.), PET 2006, LNCS 4258, pp. 152–171.

Weiss S., (2008), in Fischer-Hübner, S., Duquenoy, P., Zuccato, A., and Martucci, L. (Eds.), The Future of Identity in the Information Society, IFIP International Federation for Information Processing, Volume 262, Springer, Boston, pp. 161–171.

Petković M., and Koster, R.P. (2006), *User-Attributed Rights in DRM*, in Safavi-Naini R. and Yung M. (Eds.), DRMTICS 2005, LNCS 3919, pp. 75 – 89.