Exception Based Enterprise Rights Management : Towards a Paradigm Shift in Information Security and Policy Management

Jean-Henry Morin

University of Geneva – CUI

Jean-Henry.Morin@unige.ch

Abstract

Enterprise DRM is still dominated by vendor driven proprietary approaches fundamentally lacking interoperability features and essentially relying on strong cryptography lacking the flexibility to accommodate unanticipated work situations requiring exceptional actions. Consequently users increasingly circumvent corporate security policies just to get their work done and such incidents simply go unnoticed. From a management and security point of view this represents a risk in an increasingly compliance driven and networked economy. This paper explores the opportunity to apply an exception-based model for Enterprise DRM building on the proposition that monitoring security policies could be as effective as strong enforcement and provide more accurate information to manage and tune corporate digital policies.

Keywords: DRM, Exception Management, Monitoring

1. Introduction

This study draws on two research streams in the field of DRM. First in the media DRM sector trying to address the hard problem of managing rights for digital artifacts in ways allowing to accommodate for fair use (i.e., supporting the Copyright Balance Principle [1]). Second in the Enterprise DRM sector where these technologies gained much visibility following corporate scandals to help address governance, risk and compliance issues (GRC) [3].

The key question underlying this study stems from exactly the same initial questions raised in the media sector. Namely, is Enterprise DRM (and by extension information-centric security) following the wrong path with the wrong assumptions? This is what led to designing a model for managing exceptions in DRM environments [3] hypothesizing that the users weren't criminals *a priori*. Both areas appear to share similar properties but for different reasons. The main contribution of this paper is to raise the issue in similar terms in the corporate sector and to propose applying our model in Enterprise DRM environments as a feature enabling better usability and efficiency, increased traceability and monitoring of legitimate uses instead of untraceable security policy circumvention and ultimately a way for security professionals to tune policies based on real usage patterns.

This paper is structured as follows. After further describing the problem, section 2 presents the Exception Management model. The application of the proposed model is discussed in section 3. A possible architecture is described in section 4. Section 5 outlines related work. Concluding remarks and future work are presented in section 6.

1.1. Issues and objectives

While the market of information-centric security has now matured to a point where Enterprise DRM is a known technology, this industry is still struggling with interoperability issues. Solutions are still proprietary, offering limited mechanisms for generic interoperability among them. Assuming organizations increasingly need to engage in ad-hoc, short-lived and dynamic collaborations requires these systems to be able to accommodate such exchanges across organizations not necessarily having the same Enterprise DRM system.

While this is a critical issue and an enabling factor for the broad endorsement and deployment of Enterprise DRM based systems, there still remains a hard problem to be addressed. How do DRM enabled systems manage or are able to deal with so called exceptions? In order to further emphasize this critical issue, let us illustrate this issue in the media sector before transposing it to the corporate environment.

Let's start with the *Copyright Balance* principles that should underline public policy regarding DRM as proposed by E. Felten in a column of CACM [1]: "*Since lawful use, including fair use, of copyrighted works is in the public interest, a user wishing to make lawful use of copyrighted material should not be prevented from doing so by any DRM system.*". This sound principle is exactly at the forefront of our work making the case for such "Exception Provisioning" in DRM enabled systems.

Drawing on this principle and applying it to the corporate environment for information security leads to defining the *Enterprise Security Balance Principle* :
"*When legitimate use of, or access to, managed or secured corporate resources is in the interest of the company, an employee or business partner wishing to do so should not be prevented from doing so by any Enterprise DRM or security system.*"

Now, contrary to the initial principle that applies essentially to the media and entertainment sector with respect to lawful and fair use rights any individual may claim, the above-derived principle is idealistic and irresponsible given the much different nature of corporate resources. As a result we need to augment it with an additional property. Namely requiring that an auditable trace be systematically logged. Consequently, the revised *Enterprise Security Balance Principle* becomes:

"*When legitimate use of, or access to, managed or secured corporate resources is in the interest of the company, an employee or business partner wishing to do so should not be prevented from doing so by any Enterprise DRM or security system provided an auditable trace be systematically logged.*"

To further support our proposition and our assumption, let's review a few facts and figures from the industry. There is very little evidence about circumvention of corporate security policies for obvious reasons that in most cases such incidents go unnoticed unless problems occur thus revealing the incidents. However, recently these questions appear to be increasingly studied in the light of risk and compliance issues. For example, a recent survey from EMC's RSA security division [4] shows interesting results. According to the survey, 53 % admit working around corporate security policies just to get their work done. Another interesting figure comes from a Cisco white paper based on a survey conducted among 2000 IT professionals in 10 countries [5] reveals among the top reasons for violating corporate IT policies are that (a) it doesn't match the reality and what is needed to do their job, (b) they need to access applications not included in the company's IT policy to get their job done.

Such figures are clear indications of a problem and mismatch between corporate security policies and the actual day-to-day operations where regular employees are led to circumventing these security policies just to be able to accomplish their work. What does this mean for the employees, the company and security professionals?

For the employees, we can clearly imagine the amount of extra burden put on them in situations where they ultimately need to be "creative" to do their job. Consequently, this lack of usability may lead to additional stress with respect to their responsibility when "breaking the rules". Moreover, this leads to additional inefficiencies and most importantly untraceable policy transgressions. All this has a direct cost for the company in addition to the increased level of risk for the company (e.g., data leakage, compliance, undocumented actions, etc.). Ultimately, the security professionals have no way to monitor such incidents in order to evolve and tune corporate security policies according to the actual needs of the company and its employees.

This in turn raises another question about the underlying assumption of corporate security. Until now, most of the enterprise security is following a "closed" model whereby anything that isn't explicitly authorized is forbidden. Enterprise DRM follows the same pattern basically persistently protecting content using strong cryptography thus forcing employees to potentially circumvent security policies and procedures in order to accommodate day-to-day operations that oftentimes haven't been anticipated and factored in the policies. Such examples are numerous and include sharing passwords and accounts, using removable media, etc.

This approach suffers from the same limitations found in the media DRM sector criminalizing the user / employee by default. In other words, not trusting him. We argue that one should put back the trust where it belongs. Shouldn't employees be trusted unless otherwise witnessed? By all means, if a company has employed someone, it has placed trust in this person. When an employees' judgment commands to do something, he usually is accountable for it. Now, using backdoors definitely worsens the problem while one might simply argue that if an employee claims he needs to do something, he knows best.

This is exactly the motivation behind the idea of introducing exception management in Enterprise DRM. Anyone claiming he has the right to do something should *a priori* be trusted provided he is willing to leave a trace for monitoring and accountability. This represents a major paradigm shift in how we approach security. Most people are trustworthy and consequently security shouldn't be a constraint (enforced) but rather a help (monitoring).

1.2. Using Credentials for Exceptions

Our approach is based on using some form of credentials whereby a DRM module would provide an entry point to evaluate locally held credentials that could have precedence over the attached rules and be traceable (i.e., auditable). The process could be rather straightforward as it would be comparable to the existing verification of locally held licenses in the users' license-store. For example, let's imagine that a new employee is provided with such a credential showing he is affiliation and status together with other administrative tokens. Such credentials would be stored on the users computer (e.g. in a credential store) and made available to the DRM module (enforcement point) when evaluating rights at runtime.

This rather elegant approach allows to potentially handling many situations where explicit policy specification would simply be too cumbersome or simply impossible to anticipate and formalize. In the case of fair use, it is commonly agreed that non-commercial use of copyrighted material in academic environments is free. Being a faculty or a student would allow having an academic credential delivered by the university.

In a general way, such an approach allows to capture generic rights management in the form of groups or communities. Being a member of a group provides a generic right with respect to content when accessed by its members. Further refinement could consider a hierarchy of credentials for example within a company where management would be provided credentials with broader rights than those of staff members.

2. The Exception Management Model

The proposed model presented in detail in [3] involves two additional entities to traditional DRM based environments: a Credential Manager and an Exception Manager.

The Credential Manager is an entity that emits, revokes and manages credentials. It can be any structure, such as an enterprise, an academic entity, or a national entity. It does not have to be known by the Content Owner neither at credential generation time, nor at content creation time; but it has to be able to prove its legitimate existence as well as the motivation leading to generating credentials.

The Exception Manager is an extension of the traditional License Manager found in all DRM based environments. It verifies if a credential may qualify to give access to a piece of rights enabled content. The Exception Manager checks if the credential is valid, if it has not been revoked and if it may be applicable to the content. Thus it verifies if the Credential Manager has legal existence and evaluates the reasons that led to generating the specific credential. If the credential passes these verifications, a Short-Lived License may be granted providing access to the content for a limited time. Moreover, the operation is logged as a trace for further proof of legitimate activity. Short-Lived Licenses are thus meant to give an exceptional access to content, and their validity is thus limited in time. They can give more or less rights depending on the type of the detected exception and some optional metadata information attached to the content indicating specific constraints on the Short-Lived License.

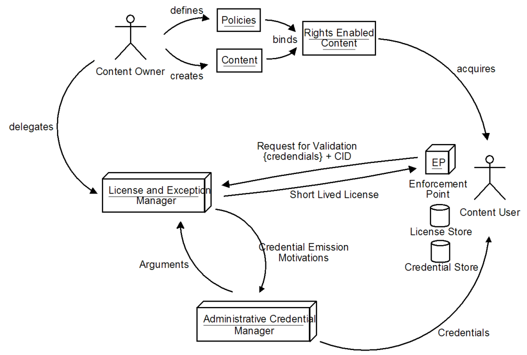

Figure 1. Exception-based Model.

As a general overview of the model, Figure 1 highlights the main difference with a traditional DRM model. First, the content users obtain credentials from Credential Managers. These credentials are then stored in a credential store alongside the local license store to be used by the enforcement point. Compared to a classical DRM model where the enforcement point only has the choice to grant or denying access or eventually try to acquire a license, in the credential based model, credentials held by users can be sent to the exception manager and used to check if the user qualifies for an exception. If so a corresponding Short-Lived License is issued and returned for use.

As a result, content protection, credential creation, exception verification and corresponding authorization are decoupled. This approach provides greater flexibility than the classical DRM model allowing Credential Managers unknown to content owners to inform Enforcement Points that an exceptional situation may be taken into consideration in situations where the user has no explicit rights to access the content in the form of a traditional license.

While providing flexibility to content users this approach still gives final control to the Exception Manager by allowing it to verify several points mentioned above leading to evaluating the legitimacy of the requested exception. Content Owners only have to care about the way they wish to protect their assets, ad hoc decisions being taken by the Exception Manager in case of exceptional situations. Finally, based on the logs of the credential manager the content owners can request audits of these logs either in case of fraud suspicion or simply as a regular validation procedure of the credential manager.

Lets now describe in further details the credential based model for managing exceptions in DRM systems. We first present the specifics of the content protection process when using exceptions before describing the exception management itself.

2.1. Content protection

Content protection in the context of an exception based model differs from its traditional representation. This section explores the main differences introducing or refining the concepts of core policies, certification delegation, exception handling delegation and rights distribution.

Core Policies. At the very beginning of the content protection process the definition of policies is driven by the need to protect a content asset. But this process follows a path leading from this simple content protection to the need of having flexibility in any situation. Following this path results in producing complex policies required to deal with all particular situations that may arise.

In the proposed exception based model, only core Policies should be associated to content. Core Policies are the set of policies needed to efficiently protect the content in most situations. These policies have to reflect enterprise strategy, the most important requirements concerning the content and all usual situations that may occur. Thus policies embedded into the rights enabled content should not include other considerations, such as policies dealing with extremely rare situation consequently considered as exceptions.

In this context all policies added to provide further flexibility not in the scope of usual policies are considered as potentials exceptions and should thus be handled using the credentials based exception handling model.

Credential Properties. Credentials have the following set of properties:

Known Source: Credentials must contain information about the Administrative Credential Manager who generated them, in order to be able to verify its legal existence as well as the motivations that led to credential generation.

User Bound: Each credential is bound to a single user or role, affiliated to the Administrative Credential Manager, able to prove that he is the legitimate owner of the credential.

Limited validity: Credentials are limited in time; their validity period is included in the credential.

Revocable: The Administrative Credential Manager can revoke a credential it has generated at any time.

Note that information about the nature of the credential, the reasons explaining why it has been created are not embedded into the credential. This approach allows to modify the scope of credentials generated by an Administrative Credential Manager for a single user, by widening the set of motivations, narrowing it or refining it, without having to revoke the credential and having to generate new ones. This provides additional flexibility, while retaining control over the number of credentials.

Credential Generation. In the model, generation of credentials that may lead to exceptions is delegated to Administrative Credential Managers. This indicates that credential owners can legitimately ask for the rights to access a piece of content in a given context.

Resulting credentials do not provide any direct access grant to a piece or type of content, but only indicates that even if their owner does not have the rights - in the form of a license - to access a piece of content and if the credential is recognized, he may be entitled to the right to access the content due to an exceptional situation.

Exception Handling Delegation. As stated before, the goal of the credential based model is manifold. First, it provides a way to reduce the complexity and size of rights and policy managed contents. Second it provides more flexibility in handling special or unanticipated situations as content needn't be modified to deal with such situations. Finally, it simplifies the role of content owners allowing them to produce contents and protect them with the most important and representative policies, not having to deal with all possible situations.

As a result, businesses are provided with a flexible way to delegate handling of particular situations potentially allowing exceptions. In this model, exceptions are detected, verified and handled by an Exception Manager not involving directly the content producer, nor having to modify the content in order to adapt to new exceptional situations. Activity logging is done for further audit by interested parties.

2.2. Exception management

In this section we explore in further details the process of rights verification, exception detection and short lived license acquisition.

Rights Verification. A central role in the proposed exception based model is the rights verification process. As stated before, the way the enforcement point manages rights verification in our model differs from the usual way. Figure 2 depicts the underlying sequence of actions that have to be completed.

When a user wants to access content (1), the held licenses are taken from the users' license store (2) and the enforcement point tries to use them for the requested action (3). This part of the process is exactly the same as done traditionally. If existing licenses match content policies, access is granted (4a). If none of the licenses are applicable to the content, available credentials are taken from the local credential store (4b) and content identification is extracted (5). These information are signed and sent (6) with the information about the way the content is being accessed, to the Exception Manager for further verification (7). This next step tries to detect possible exceptions instead of simply denying access to the content. The enforcement point then waits for an answer which can eventually be a short lived license, if an exception is considered, and uses it (8) to then grant access to the content (9) and store the license (10) or a deny if not (11).

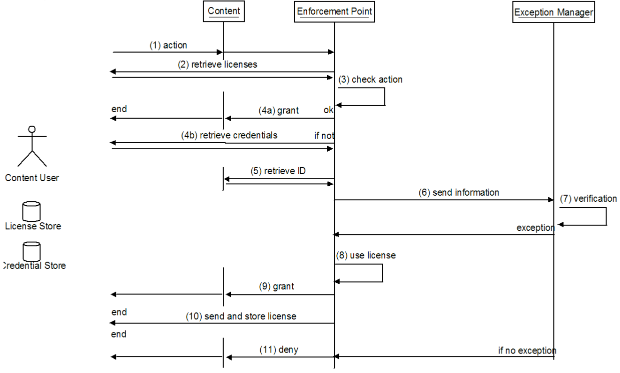

Figure 2. Rights Verification Sequence Diagram.

Exception Detection. When the exception manager receives the credentials, as well as content identification and the usage context, it tries to detect if a suitable combination is applicable for an exception. For each credential multiple steps are involved. These are illustrated in Figure 3.

First, the exception manager has to verify if the credential has been generated by an existing and valid Administrative Credential Manager (1). To achieve this task, the credentials have to be examined in order to retrieve information about their creator, and then verify their legal existence. The next step is to verify if the credential really belongs to the user trying to access the content (2). If it is the case, the exception manager checks if the credential is still valid (3) and asks the credential manager if it has not revoked it (4). Administrative Credential Manager verifies it (5), and then sends an answer (6). Credentials not complying with any of these rules are ignored (7). Last step is then to check if the credential can be applied to the content in the context in which the content is to be used. To do so the Exception Manager asks the Administrative Credential Manager for the motivations that have led to a credential generation (8) and the Manager sends back its signed answer (9). This answer may include textual information that can be analyzed, parsed; it may also contain any other kind of information such as a certificate emitted by a content owner indicating that a contract has been signed by both parties, or even another credential emitted by another recognized Administrative Credential Manager. If this last verification succeeds - i.e., if any of the retrieved information is accepted (10) - an exception is applicable and the short lived license acquisition process can start (11). When all credentials have been verified, a short lived license or a deny is sent back to the enforcement point depending on the result of the process (12).

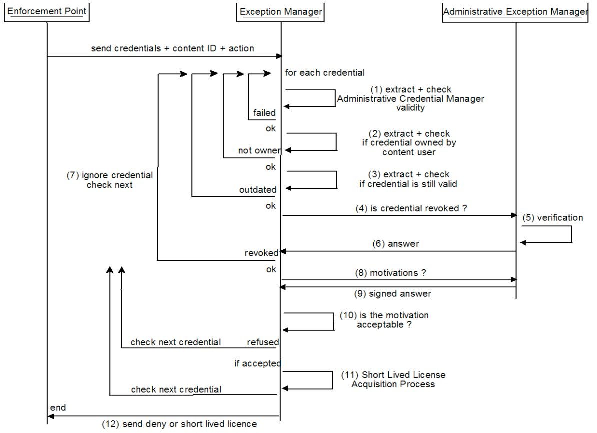
Enforcement Point
Exception Manager
Administrative Exception Manager
send credentials + content ID + action
for each credential
(1) extract + check Administrative Credential Manager validity
failed
ok
(2) extract + check if credential owned by content user
not owner
ok
(3) extract + check if credential is still valid
outdated
ok
(4) is credential revoked ?
(5) verification
(6) answer
revoked
(7) ignore credential check next
ok
(8) motivations ?
(9) signed answer
(10) is the motivation acceptable ?
check next credential
refused
if accepted
(11) Short Lived License Acquisition Process
check next credential
end
(12) send deny or short lived licence

Figure 3. Exception Detection Sequence Diagram

Short Lived License Generation. The short lived license generation process is started when an exception has been detected and is applicable. This is a recursive process creating a license based on all exceptions that have been detected as applicable for a single access to a rights enabled content.

At this stage, the Exception Manager knows that it has to deal with an exception situation and knows what credentials have raised what kind of exception. The short lived license is built incrementally analyzing all exceptions. In order to emit such a short lived license some precautions have to be taken in order to manage issues of precedence and potential conflicting exceptions.

Figure 4 presents the different steps of this process. First, each exception has to be logged for traceability purpose (1). The log has to keep all required information to justify the exception. This includes the identification of the content, the credentials that led to an exception, the motivations signed by the Administrative Exception Manager and the context of use, i.e., the foreseen type of content access. Once all required information have been logged, the rights the specific exception may grant to the user are compared to the rights granted by previous exceptions, and the license is refined (2). Differences may occur based on the provided reasons. For instance, a first credential may raise an exception with motivation "academic use", and a second credential may indicate that there is a "research agreement with the content owner". First credential would allow limited use, but second one would allow access to additional features, or a more detailed output. Once all exceptions have been handled, the short lived license can be generated (3).

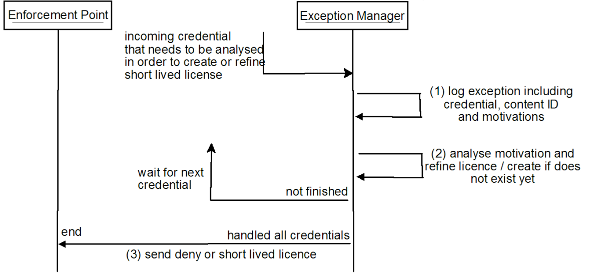
Enforcement Point
Exception Manager
incoming credential that needs to be analysed in order to create or refine short lived license
(1) log exception including credential, content ID and motivations
(2) analyse motivation and refine licence / create if does not exist yet
wait for next credential
not finished
end
handled all credentials
(3) send deny or short lived licence

Figure 4. Short Lived License Acquisition Sequence Diagram.

The log of all exceptions is needed in order to be able to detect Administrative Credential Managers, or users abusing the system - and eventually blacklist them -, and keep a global trace of content usage.

The validity of the license will be usually short (from a single access to a few days validity) or with limited use (read only) as each credential can be revoked at any time. But the effective validity is a matter of specific policies bound to the content owner which may eventually also be set as a core policy attached to the content. The final decision is thus left to the Exception Manager responsible for this task.

3. Applying the Model to Enterprise DRM

Lets now put the model into perspective of Enterprise DRM. Figure 5 shows the resulting diagram.

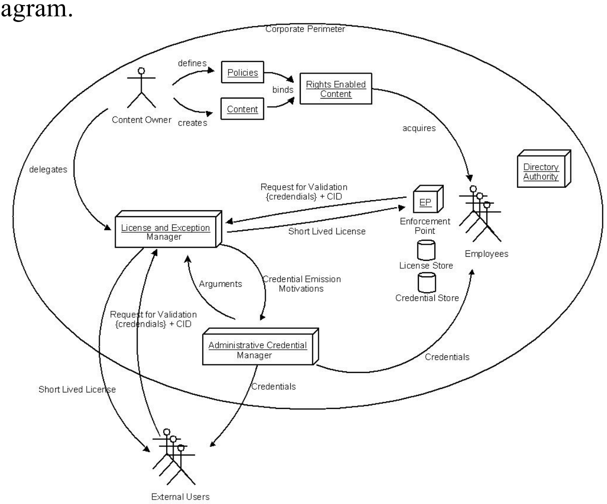

Figure 5. Enterprise Exception Based DRM

Applying it to the corporate sector appears to offer several simplifications to the model as well as some potential advantages for collaboration with external partners.

The first simplification comes from the fact that basically all the components of the architecture lie within the corporate perimeter. Content producers, owners and users are part of the same company. The only external entities being external partners with whom collaborations exist. Content producers and owners being internal production and application of policies to produce rights enabled content is much simplified. Moreover combination with enterprise wide applications and content management systems and repositories is also internal.

The DRM license server is also enterprise bound and serves the employees for all regular DRM related interactions.

Employees being part of the organization also simplifies administration in terms of having access to a corporate directory authority (e.g., LDAP, AD, etc.).

The Credential Manager is also bound to the corporate infrastructure and can easily interact with the directory authority to emit credentials for employees. It may be asked by employees to produce a Credential for an external user. In this case the credential is provided to the external user for sporadic uses on a case-by-case basis.

The Exception Manager is internal to the company and serves short-lived licenses to employees and external partners alike based on the provided credentials and exception requests. It may interact with the Credential Manager to request additional information when needed.

Every actor keeps a trace in logs of each transaction. This may be made available in real-time to security policy auditors through appropriate tools to monitor how effective policies are or in case alerts are set, to take prompt action in the event a malicious user attempts to do something highly sensitive. This is a powerful approach to managing corporate digital policies thus allowing tuning policies according to real usage situations. Moreover, management dashboards can be built to capture in real-time potential compliance risks.

4. Architecture Overview: Attribute Certificates

The basic idea behind the proposed approach is to make use of a credential based scheme. This raises however the issue of who and how these credentials are managed. To this end, we propose the use of PKI infrastructures which are already well established techniques. Moreover, certification authorities are accustomed to handling similarly sensitive aspects of security. The model would also perfectly fit the operation of such services with registration authorities, issuing services, revocation lists, etc.

Instead of using X.509 public key certificates (PKCs), we propose to use X.509 Attribute Certificates (ACs), RFC3281 [6], having a similar structure to PKCs without the public key. ACs can hold attributes specifying relevant information such as roles, affiliations, temporary situations or whatever is needed to evaluate exceptions.

Such credentials would be delivered to the user, together with other administrative tokens, passwords, etc., by the institution / organization to which the user is affiliated. A credential would hold several information such as a known lifetime (expiry date), a unique ID (affiliation, employee number, etc.) within the domain of the institution delivering the credential, and any other relevant information that should be used when evaluating whether or not an exception or waiver is applicable.

From thereon, the DRM system, upon deciding whether or not to render the content, could be required by the user to first check for locally held credentials. Then based on these credentials, further actions could be undertaken in order to acquire the corresponding license and thus grant the user access based on his situation. The important point to note here is that basically the content remains persistently protected. It is processed just as if it were in a situation without exception request. The rendering is done within the usual trusted renderer and basic rules, identified as mandatory for example can still be enforced. A proof of concept prototype was implemented and discussed in [26]

5. Related Work

To the best of our knowledge, we have not been able to find any related initiative in Enterprise DRM as it is considered to defeat the purpose. In this section we focus on highlighting projects, DRM standards and architectures that not only consider DRM from the content owner's perspective, but also from the consumer's viewpoint. A more detailed overview of DRM evolution and key contributions, which have led to consider such issues, can be found in [7].

DRM raises issues involving different interests thus leading to often incompatible requirements of actors in the value chain. While most existing DRM solutions are content provider centric and are meant to protect their rights, there has been little attention given to the consumer side of rights management. In order to raise awareness, help reconcile these interests and to support the emergence of a common European position with respect to consumer and user issues of DRM solutions, the EU INDICARE project [8] was launched. It aimed at investigating issues like consumer acceptability of DRM systems, their interface and functionality, as well as policy issues linked to privacy and access to information. One of the main outputs of the project was its Consumer's Guide to Digital Rights Management, published in ten European languages. This guide provides concise, neutral and understandable information about what DRM is and why it matters to consumers.

The disruption to rights balance is currently illustrated by the fact that currently most DRM solutions bind content to hardware devices physically; while such an approach provides straight-forward security for content owners, it cruelly limits content usage by preventing often legitimate behaviors such as space shifting (i.e., ability to transfer content among devices) and fair use rights traditionally enjoyed for decades now. To tackle this issue, Sun Microsystems introduced Project DReaM (DRM everywhere available) [9], a project to create an open-source standard for interoperable DRM that relies on user authentication alone rather than devices. Project DReaM includes the DRM-OPERA architecture and makes it available in the form of an open-source community Java development project.

DRM-OPERA is an open DRM architecture [10] aiming at enabling the interoperability between different DRM systems. It has been specified and prototyped within project OPERA of the Eurescom organization. Among other activities, the OPERA project has produced an overview of state-of-the art DRM systems and standardization activities as of 2002 [11]. The DRM-OPERA architecture offers two interesting features that differentiate it from other solutions. First, it makes usage licenses independent of the underlying DRM system by offering its own license management. Then, usage licenses are bound to users instead of, as it is common with existing solutions, to devices.

While DRM future was discussed in silos across the industry be it consortiums like Coral [12] or standard initiative like DMP [13], there was no place where the whole community of all of the digital content stakeholders could come to discuss, define, and develop the future of digital content and DRM. To tackle this issue, Sun Microsystems decided in August 2005 to provide a virtual meeting place for all those contributing to this effort by creating the Open Media Commons [14], an open source community project, and a tool by sharing the internal project DReaM with the community under the OSI-approved Common Development and Distribution License (CDDL). One of the aims of the Open Media Commons community is to create an open environment where creators, content owners, consumers, network operators, technology providers and consumer electronics device manufacturers can work together to address the technical problems associated with DRM [15].

The Marlin Joint Development Association [16], is a consumer electronics industry technology development alliance formed by Intertrust Technologies, Matsushita Electric Industrial (Panasonic), Royal Philips Electronics, Samsung Electronics, and Sony Corporation that aims at creating a set of specifications for an open standard interoperable DRM platform for consumer electronics. In order to provide interoperability of content whatever distribution mode, DRM technology and standard are used, Marlin JDA specifications aim at providing a single technology toolkit to build DRM functions into their devices to support commonly used content distribution modes and thus avoid conflicts due to proprietary DRM technologies and standards. Marlin's authentication is user-based: it defines that user should be able to use content on any device they own and thus that content be tied to user identities and not device identities. While hiding issues such as content and device ownership that will need to be tackled, such a design is a step towards the copyright balance as defined previously. Marlin JDA is closely related to the Coral Consortium and as such, Marlin-based devices are able to interoperate with Coral-enabled DRM systems even if those systems do not use Marlin DRM components. It relies on Intertrust's NEMO [17] and Octopus technologies [18].

The Digital Media Project [19] is an independent standards initiative lead by Dr. Chiariglione, the founder of MPEG, aiming at tackling specific issues of DRM environment mainly related to the balance between content owner and consumer rights. The DMP defines its mission as being to "promote continuing successful development, deployment and use of Digital Media that respect the rights of creators and rights holders to exploit their works, the wish of end users to fully enjoy the benefits of Digital Media and the interests of various value-chain players to provide products and services" [19]. The project standardizes appropriate protocols aiming at supporting the functions value-chain users need to execute and provides an Interoperable DRM Platform (IDP) specification [20] derived from MPEG-21 [21] standards and including an extended subset of MPEG-REL [22]. The IDP is based on requirements that have been derived from three sources, and which the platform has to be able to represent. The first one, Traditional Rights Usages (TRUs) covers usages exercised by media users and enjoyed in the pre digital era. The second one, Digital Enabled Usages (DEU), are usages either not possible or not considered in the analog domain. Finally the Digital Media Business Models (DMBM) is a set of TRUs and DEUs assembled to achieve a goal.

Other research works aim at proposing solutions to protect the copyright in a balanced way for copyright holders and users. The problem of managing exceptions is considered a hard problem and has been mainly explored in the context of fair use and rights expression languages. For instance, in [23], authors explore how rights management systems can be designed and implemented in a way that preserves the traditional copyright balance, especially with copyright's concern for the public domain and for the legitimate fair use. The authors are against leaving the determination of fair use in the rights holder's hands. Indeed they emphasize the fact that collective public interest may run contrary to the rights holder's individual interest and thus there may be a strong incentive for the rights holder to deny access. The authors doubt that system designers will be able to anticipate the range of access privileges that may be appropriate to be made of a particular work.

The analysis led in [24] suggests certain accommodations that DRM architectures, and especially their rights expression language components, should make to adequately express certain core principles of copyright law. Authors make two recommendations. The first recommendation proposes changes to the XrML REL vocabulary [25] to be able to highlight limitations on copyright exclusivity in cases such as fair use or first sale and rights transfer situations. The second one, goes toward the need for the creation of an Open Rights Messaging Layer. Indeed, their paper highlights current lack of rights messaging or transaction protocol that would provide standardized means for retrieving and disseminating rights information and policies, and issuing rights grants or permissions.

The details describing how these approaches relate to the model underlying the implementation presented in this paper are further discussed in [3]. In summary, it is legitimate to state that exception management in DRM systems remains an open question.

6. Conclusion and Future Work

This paper proposes a paradigm shift in information-centric security by expanding to the corporate sector work done on exception management in DRM environments. We argue that monitoring as an alternative to strong cryptography-based information security could provide increased efficiency while still preserving the much needed monitoring and tracking required in increasingly regulated environments where governance, Risk and Compliance issues are critical.

As a corollary, given such an approach, it would provide security policy professionals with a much needed feedback on security incidents and circumventions that are most often unnoticed today.

To this extent we argued for the need of an Enterprise Security Balance Principle whereby employees should be more trusted and given the flexibility to officially force security policies without having to unlawfully circumvent them based on their judgment. Since all actions are logged, security policy auditing and evolution becomes an added feature of the approach.

Further research and data is needed to validate our assumptions on security policy circumvention and the efficiency / usability issue. A prototype implementation of the approach in the context of a real Enterprise DRM system is a necessary step towards advancing our work.

Finally, recent evidence based on a study conducted in South Korea [27] suggests that among the major drivers of organizational adoption of Enterprise DRM, Compliance might not be the primary factor. While identified as being among them, it appears that Knowledge Management (KM) and Inter-organizational Structures (IOS) rank higher. In which case, following the adage “what can do the most can do the least”, if sound rights managed KM and IOS embodies monitoring and audit trails compliance could be a “built-in” feature. Further study is needed to validate these propositions.

References

[1] E. Felten, “DRM and Public Policy”, in Communications of the ACM, V. 48, No. 7, July 2005, p. 112.

[2] J.-H. Morin and M. Pawlak, “Towards a Global Framework for Corporate and Enterprise Digital Policy Management”, in Journal of Information System Security (JISSec), G. S. Dhillon (Ed.), 2006, Vol 2, No. 2, ISSN 1551-0123, pp. 15-24.

[3] J.-H. Morin, M. Pawlak, "A Model for Credential Based Exception Management in Digital Rights Management Systems", in proceedings of First International Conference on Global Defense and Business Continuity, ICGD&BC 2007, Second International Conference on Internet Monitoring and Protection, IEEE, July 1-6, 2007, Silicon Valley, USA.

[4] RSA Security, “The 2008 Insider Threat Survey”, Oct. 2008.

[5] Cisco Systems Inc, “Data Leakage Worldwide: The effectiveness of Security Policies”, White Paper, Aug. 2008.

[6] S.Farrell, R.Houslez, RFC3281, Internet Society, Apr 2002

[7] J.-H. Morin and M. Pawlak, “From Digital Rights Management to Enterprise Rights and Policy Management: Challenges and Opportunities”, chapter 9 in Advances in Enterprise Information Technology Security, F. Herrmann and D. Khadraoui (Eds), Information Science Reference, IGI Global, July 2007, pp 169-188.

[8] INDICARE. The Informed Dialogue about Consumer Acceptability of DRM Solutions in Europe, from http://www.indicare.org/

[9] Fernando, G., Jacobs, T. and Swaminathan V., “Project DReaM An Architectural Overview”, White Paper, Sun Microsystems, Sept. 2005.

[10] EURESCOM P1207 OPERA, An Open DRM Architecture. from http://www.eurescom.de/public/projectresults/P1200-series/P1207-D2.asp

[11] EURESCOM P1207 OPERA, Overview of state-of-the art DRM systems and standardization activities, from http://www.eurescom.de/public/projectresults/P1200-series/P1207-TI.asp

[12] CORAL Consortium Corporation, from http://www.coral-interop.org/

[13] DMP, Digital Media Project, from http://www.dmpf.org/

[14] OMC, Open Media Commons, from http://www.openmediacommons.org/

[15] Open Media Commons FAQ’s, from http://www.openmediacommons.org/faqs.html

[16] Marlin JDA, CE and DRM Technology Leaders to Create a DRM Toolkit for Consumer Devices, from http://www.intertrust.com/main/news/2003_2005/050119_marlin.html

[17] Bradley, W.B. and Maher, D.P,. The NEMO P2P Service Orchestration Framework. In IEEE (Ed.), 37th Hawaii International Conference on System Science. IEEE.

[18] Intertrust, Octopus Principles of Operation. Internal Memo.

[19] DMP, Digital Media Project, from http://www.dmpf.org/

[20] DMP, Digital Media Project. Approved Document No 3. Technical Specification: Interoperable DRM Platform, from http://www.dmpf.org/open/dmp0653.zip

[21] MPEG-21 Multimedia Framework, from http://www. chiariglione.org/mpeg/standards/mpeg-21/mpeg-21.htm

[22] MPEG-REL, Multimedia framework (MPEG-21), Part 5: Rights Expression Language, from http://www.iso.ch/iso/en/CombinedQueryResult.CombinedQueryResult?queryString=21000-5

[23] D. Burk, J. Cohen, Fair Use Infrastructure for Copyright Management Systems, 11 Harv. J. Law & Tech., 2002.

[24] Mulligan, D., Burstein, A., and Erickson, J. "Supporting Limits on Copyright Exclusivity in a Rights Expression Language Standard. A requirements submission to the OASIS Rights Language Technical Committee.", Samuelson Law, Technology & Public Policy Clinic, and The Electronic Privacy Information Center, August 2002.

[25] XrML, eXtended rights Markup Language, from

[26] J.-H. Morin and M. Pawlak, “Exception-Aware Digital Rights Management Architecture Experimentation” in proceedings of 2008 International Conference on Information Security and Assurance (ISA 2008), IEEE, April 24-26, 2008, Busan, Korea, pp. 518-526.

[27] J.-H. Morin and A. Zeelim-Hovav, “Strategic Value and Drivers behind Organizational Adoption of Enterprise DRM : Setting the Stage”, in proceedings of 7th Annual Security Conference, Las Vegas, NV, USA, June 2-3, 2008.