Towards DRM/DPM enabled interoperable Enterprise Information Systems

Michel Pawlak,
Michel.Pawlak@cui.unige.ch

University of Geneva
Centre Universitaire d'Informatique
Geneva, Switzerland

Abstract. Modern enterprise information systems are heterogeneous environments combining resources coming from different sources. Multiple domains are involved, and as such the ability of information systems to be interoperable, the ability to ensure persistant security as well as the ability to reflect the dynamics of the corporate environment are mandatory. The definition and management of static access rights through access control lists dispatched accross multiple and evolving environments is difficult and not sufficient anymore. Further, information systems are now expected to ensure regulatory compliance. In this context, security of information systems has to be extended and adapted to provide an interoperable global security environment, reflecting strategical security needs and applying them at the operational level.
This paper discusses how Digital Rights and Policy Management can enable interoperable and dynamic policy driven security and presents the benefits of such a global interoperable security scheme over traditional security schemes.

1 Introduction

Nowadays, modern enterprise information systems are an interconnection of heterogeneous systems like frameworks, knowledge management systems, enterprise resource planing, databases, datawarehouses, etc. Resources can be distributed over multiple sites belonging to different companies. Different technologies and approaches are used to access these resources, to communicate and provide service like web services or mobile agent systems. Involved processes have to cross these heterogeneous systems and be able to to adapt to the different security schemes and authentification systems that may be combined. Thus resource security and security interoperability are extremely important issues.

Further, currently, increasing emphasis is put on regulatory compliance. For instance Sarbanes-Oxley Act (SOX [1]) auditors can demand to see auditing records of virtually all computer access. This increases the need for adapted security solutions to control access to enterprise sensitive ressources. SOX is a first glance of how economical and legal environments will influence tomorrows enterprise information systems.

Future information systems will have to be able to reflect strategical issues like corporate governance, compliance, liability, policies, etc. Information systems will have to be able to capture and apply these issues at an operational level, in order to ensure valid system execution. Moreover, to constantly reflect reality, future information systems will have to be able to evolve dynamicaly with the environment. In this context, issues concerning persistent protection of ressources, adaptable policy driven control of distributed ressources and interoperability are not disjoin domains. Traditional security approaches through static control access lists are not sufficient anymore.

Nevertheless, interoperability does not only concern IT and IS related issues. Aligning the business and enterprise strategy with IT and IS issues is where future interoperability issues reside. Flexibility, adaptability, persistent security and precise representation of enterprise strategical and legal environment are needed, and have to be represented in a common *global security* scheme.

The goal of this paper is to show how Digital Rights and Policy Management (DRM/DPM) driven security can be used in order to offer a global solution tackling these issues.

This paper is structured as follows. Section 2 details how DRM/DPM can provide interoperable security. Some other existing approaches ar discussed in section 3. We present ongoing work in section 4 and we finaly conclude in section 5.

2 Security interoperability through DRM/DPM

This section presents how Digital Rights and Policy Management can enable interoperable security and how their use covers security needs from both strategic and operational point of view.

2.1 Enterprise Digital Rights and Policy Management

With modern Enterprise Information Systems, enterprise processes have to span accross multiple corporate structures. In this context the issue of persistent content protection, rule based access to content and usage metering appear as key requirements. In order to protect themselves, enterprises have to deal with the recurring problem of managing, safeguarding and controlling usage of information assets wherever it resides and especially outside the corporate firewall. The technology addressing this security issue is called Digital Rights Management (DRM) and its strategic managerial dimension is called Digital Policy Management (DPM). As a result, any attempt to access a content protected by DRM requires interpreting associated rules prior to granting or denying the right to do so [2]. Enterprise DRM and Enterprise DPM, are the application of DRM/DPM to the corporate environment in order to protect any kind of corporate informational resource.

One of the major problems that hampered broader and faster adoption of DRM was the lack of standards and the totally incompatible proprietary solutions that were available (e.g., Microsoft, InterTrust, ContentGuard, IBM,

etc.). Nevertheless, associations like OMA (Open Mobile Alliance) [3] or MPEG-21 [4] are actively working on DRM standardization and the situation is progressively changing. Recently ISO ratified two sandards developed within MPEG-21 : MPEG-REL (ISO/IEC 21000-5:2004), a Rights Expression Language based on XrML [5], and MPEG-RDD (ISO/IEC 21000-5:2004) which addresses the issue of rights interoperability and semantics through RDD (Rights Data Dictionary). Reference implementations for both MPEG-REL [6] and MPEG-RDD [7] are currently available. Such initiatives are instrumental in this field and represent a prerequisite for broader adoption and interoperability.

2.2 Security meeting strategical and operational needs

As specified earlier, policy management is a key strategic issue for the Enterprise. Information is a corporate asset and is therefore bound to corporate policies. Companies need to be able to define and control who, how, when, what, in what context, and under which condition enterprise resources can be accessed and used at all time. These resources can be of any type like financial statements and reports, design documents, technical specifications, proposals, contracts, legal documents, emails, etc. Moreover, not only *documents* need to be protected. Processes, executable code, raw data, and value added information provided by databases and application servers, dynamically generated and which do not exist statically but are the result of specific queries are also bound to usage rights and policies.

Basic security notions providing confidentiality, authentication, integrity and non repudiation are still needed but not sufficient anymore. Digital Policy Management is of strategic nature and as such must be initiated and driven by corporate managers and not IT / IS people. It has to take into consideration three different but coexisting views : the legal environment, specific regulatory frameworks often sector bound and internal corporate policies.

Enterprise DRM meets Enterprise DPM at this point. It requires to address the issue in an interdisciplinary space between technology and management science, having to apply at the operational level decision taken at the strategical level.

2.3 DRM/DPM driven interoperable and dynamic security

Regards to information systems security, following observations can be made. First, security policies defined at a strategical level have a global validity. Regardless of the way information systems are implemented these policies have to be respected at operational level. Second, as described before, monitoring and tracability ability are an important part of modern information systems security needs. Further, rules defining if a resource (any kind of data or any system functionality) should be accessible or not depend on the context in which the ressource is accessed. As information systems are heterogenous, security interoperability is needed to provide a global view of the security context.

In order to provide more flexible and adaptable security as well as interoperability, traditional access control lists (ACL) could be replaced by DRM/DPM. Unlike ACLs wich are a static definition of access rights, DRM provide dynamic interpretation of rules, granting or denying access to resources depending on the result of a verification process. These rules can define who, how, when, for how long, can access what resource in what context.

Credentials are emited for well defined users or processes by a certified entity, granting access to functionalities and resources of the system. When a ressource is accessed, the process accessing the resource has to provide a set of credentials. The system checks if these credentials match the rules associated to the protected resource and decides to grant access to the resource or not to do it. Credentials can also be dynamically revoked if needed, for instance in case of abusive behavior, or refined to grant access to more resources.

Global security interoperability can be provided using sets of credentials. These can be used to access any resource anywhere on the information system. There is no need for the different systems to understand every credential a process provides. Once the rules mediating access to a resource are set, only relevant credentials have to be recognized. If a credential is not known, the system has to be able to check if this credential is equivalent to a known type of credentials. Such an interoperability of credentials can be achieved using standards like MPEG-RDD.

As stated before, the rules are defined at the strategical level and have to reflect strategical environement evolution. Using DRM/DPM, security can be dynamicaly refined with no need to modify already emited credentials but only by modifying the set of rules affected by the environmental change. Changing the rules has a global impact, avoiding the risk to forget to modify the rights of one given human user or process.

As each credential is affected to a particular process or user, and as the whole security scheme is based on a dynamic verification of credentials towards rules, tracability or even real-time monitoring tools can be easily implemented. Such tracability can be used to capture the context and information flow that has led to a particular access to a resource. The verification engine could then use such information to check higher level rules covering multiple aspects of the system.

3 Other approaches

Two main approaches are in use in order to tackle issues related to the authentication on multiple interconnected enterprise systems : *password synchronization* and *single sign-on* (SSO). None of these approaches tackle security issues in their globality, from the strategic, operational and interoperability point of view.

Password synchronization's goal is to ensure that when a user changes his password on one system, this change will be propagated to all other accounts automatically. The user still has to log into each system independently, but he has only one password to remember. This is a simple way to have enforce users to

have unique passwords for all parts of an information system. Such an approach is inherently insecure and definitively not designed for providing global security.

Single sign-on is a mechanism whereby a single action of user authentication and authorization can permit a user to access multiple applications within the network where the user has access permission, without the need to enter multiple passwords. Single sign-on goal is to reduce human error, a major component of systems failure [8]. Existing SSO solutions propose features like the use of strong authentication, such as biometrics, enforcement of password policies, definition of enduser credentials or audit of logins. These solutions mainly focus on securing access to ressources and monitoring actions. As SSO solutions are often used in enterprise application integration solutions (EAI) (like Microsoft BizTalk Server) they do not address the issue of interoperability of different SSO solutions, nor the interoperability with systems not designed for a particular SSO solution.

Some DRM solutions make use of SSO to provide user autentication for DRM (like Fasoo [9]), but they only use DRM to ensure the security of enterprise documents, and not in order to globaly manage enterprise information systems security.

4 Ongoing Work

We are currently working on the modelisation and development of a prototype where a mobile agent platform can interact with a database using DRM (MPEG-REL, MPEG-RDD) to ensure global security. We chosed databases and Mobile Agent Systems [10] domains in order to represent an example of the heterogeneity of modern information systems.

Agents possess a set of credentials that have been emited and signed at agent creation time by a trusted entity. These credentials define the rights an agent possesses as well as in which context these rights apply. Rights can evolve in time and be refined. The ability to access to some resources or behaviours can be dynamicaly restricted. Similarliy, new rights can be obtained and extended, offering the ability to access previously restricted resources.

In parallel, rules are associated to resources provided by databases or by agents. Each access to any type of resource (database entries or agent method / service) triggers dynamic credentials verification at runtime towards existing rules. After verification, access is granted or denied. The scope of a rule is not necessarily a paricular resource. A rule can involve multiple resources and even other rules in orther to represent in which context a process tries to access a resource. Thus, rules can be directly used to specify information flows. Moreover, rules can be dynamically modified to continuously reflect policies defined at the strategical level and thus restrict or widen access to resources.

The overall goal of this prototype is to provide fine grained control on the way resources can be accessed and show how enterprise processes can be controled using DRM/DPM. Further using DRM in a global way induces security interoperability. Indeed, in this context, from the agent perspective there is no difference between the security scheme an agent has to use to access a resource

located on a database or access a resource, method, provided by another agent or any other sytem.

When accessing a resource an agent provides matching credentials. The system checks if resources can be provided depending on dynamic interpretation of existing rules. An interesting feature provided by DRM is that there is no need for global identification and management of passwords as such information can be directly encapsulated into provided credentials. Knowing who emited the credentials for whom allows to trace and monitor agent behaviour.

As every possible situation may not be anticipated by legitimate content "right holders", formalizing exaustive rules sets appears to be hardly possible. An interesting approach to explore to tackle unexpected situations is DRM Exceptions Management [11]. DRM Exceptions provide the ability to entities asking for resources to ask for a short lived Exception Licence (as a X.509 Attribute certificate) authorizing them to access needed resources. The licence being emited if and only if the exception is recognized as valid.

Other interesting aspects that have to be considered include, for instance, the ability to define and manage what processes are authorized to do with the data they use, what are the rules associated to generated information, and how and under which conditions, local (resource related) security can be delegated to the processes using them.

Nevertheless, DPM field is currently cruelly lacking models to capture, specify, express, represent and manage policies prior to any technical DRM project and deployment in a corporate environment. Thus, future research effort will also consist in finding ways to fill this gap.

5 Conclusion

Enterprise Information Systems are living heterogeneous entities. They must be able to reflect enterprise's environement and evolve with it. Enterprise information assets are of multiple types. Any kind of document, but also raw data, processes and value added data, taken and processed from existing databases and any combination of existing systems have to be protected.

As such, when designing future information systems, multiple aspects and issues have to be considered . This includes low level security, interoperability, evolutivity, tracability and the ability of enterprise systems to answer strategic questions as well as their ability to be aligned on enterprise's strategic decisions. Integrating all these views in a common viewpoint can be called *global security*.

This paper has presented how Digital Rights and Policy Management can provide *global interoperable security* for enterprise information systems, able to meet strategical security needs and able to implement these needs at the operational level.

References

1. Sarbanes-Oxley: Sarbanes-oxley act. http://www.sarbanes-oxley.com/ (2005)

2. Jean-Henry Morin, Michel Pawlak, M.O.: Enabling technologies for the interoperable enterprise. In: Workshop on Interoperability of Enterprse Systems (INTEREST), ECOOP 2004 - 18th European Conference on Object-Oriented Programming (2004)
3. OMA: "open mobile alliance". http://www.openmobilealliance.org (2005)
4. Moving Pictures Experts Group: "mpeg-21 overview v.5". http://www.chiariglione.org/mpeg/standards/mpeg-21/mpeg-21.htm (2002)
5. "ContentGuard": "extensible rigths markup language (xrml), version 2.0". http://www.xrml.org (2005)
6. ContentGuard: "mpeg-rel sdk". http://www.contentguard.com (2005)
7. RightsCom: "rights data dictionary". http://www.rightscom.com (2005)
8. Opengroup: Single sign-on. http://www.opengroup.org/ (2005)
9. Fasoo.com: "fasoo enterprise drm". http://www.fasoo.com (2005)
10. Vitek, J., Tschudin, C., eds.: Mobile Object Systems: Towards The programmable Internet. Springer Verlag, LNCS 1222 (1997)
11. Morin, J.H.: A credential based approach to managing exceptions in digital rights management systems, CCNC/CES 2005 Workshop on Digital Rights Management Impact on Consumer Communication (2005)