Diritto digitale

Digital Right Management Systems and Trusted Computing

DRM Systems and the Law

WIPO Copyright Treaty 1996:

Article 11 Obligations concerning Technological Measures:

Contracting Parties shall provide adequate legal protection and effective legal remedies against the circumvention of effective technological measures that are used by authors in connection with the exercise of their rights under this Treaty or the Berne Convention and that restrict acts, in respect of their works, which are not authorized by the authors concerned or permitted by law.

DRM Systems and the Law

WIPO Copyright Treaty 1996:

Article 12 Obligations concerning Rights Management Information:

(1) Contracting Parties shall provide adequate and effective legal remedies against any person knowingly performing any of the following acts knowing, or with respect to civil remedies having reasonable grounds to know, that it will induce, enable, facilitate or conceal an infringement of any right covered by this Treaty or the Berne Convention:

(i) to remove or alter any electronic rights management information without authority;

(ii) to distribute, import for distribution, broadcast or communicate to the public, without authority, works or copies of works knowing that electronic rights management information has been removed or altered without authority.

(2) As used in this Article, «rights management information» means information which identifies the work, the author of the work, the owner of any right in the work, or information about the terms and conditions of use of the work, and any numbers or codes that represent such information, when any of these items of information is attached to a copy of a work or appears in connection with the communication of a work to the public.

DRM Systems and the Law

European Directive 2001/29/EC: Article 6 Obligations as to technological measures:

1. Member States shall provide adequate legal protection against the circumvention of any effective technological measures, which the person concerned carries out in the knowledge, or with reasonable grounds to know, that he or she is pursuing that objective.

2. Member States shall provide adequate legal protection against the manufacture, import, distribution, sale, rental, advertisement for sale or rental, or possession for commercial purposes of devices, products or components or the provision of services which:

   (a) are promoted, advertised or marketed for the purpose of circumvention of, or

   (b) have only a limited commercially significant purpose or use other than to circumvent, or

   (c) are primarily designed, produced, adapted or performed for the purpose of enabling or facilitating the circumvention of, any effective technological measures.

DRM Systems and the Law

Digital Millenium Copyright Act 1998:

Sec. 1201 (a) (2), 1201 (a) (3):

(2) No person shall manufacture, import, offer to the public, provide, or otherwise traffic in any technology, product, service, device, component, or part thereof, that

(A) is primarily designed or produced for the purpose of circumventing a technological measure that effectively controls access to a work protected under this title;

(B) has only limited commercially significant purpose or use other than to circumvent a technological measure that effectively controls access to a work protected under this title; or

(C) is marketed by that person or another acting in concert with that person with that person's knowledge for use in circumventing a technological measure that effectively controls access to a work protected under this title.

DRM Systems and the Law

Digital Millenium Copyright Act 1998:

Sec. 1201 (a) (2), 1201 (a) (3):

(2) No person shall manufacture, import, offer to the public, provide, or otherwise traffic in any technology, product, service, device, component, or part thereof, that

(A) is primarily designed or produced for the purpose of circumventing a technological measure that effectively controls access to a work protected under this title;

(B) has only limited commercially significant purpose or use other than to circumvent a technological measure that effectively controls access to a work protected under this title; or

(C) is marketed by that person or another acting in concert with that person with that person's knowledge for use in circumventing a technological measure that effectively controls access to a work protected under this title.

The Semantic Web

Semantic Web:

- A way to describe on-line resources:
  - Metadata and ontologies
  - XML, XML Schemas, RDF, OWL (Web Ontology Lanugage)
- RDF: triplet (Resource, Property and Value)
- Possibility to express rights and duties over on-line resources

The Semantic Web

Semantic Web: An Example

```
<?xml version="1.0"?>
<rdf:RDF
xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#
xmlns:dc="http://purl.org/dc/elements/1.1/"
<rdf:Description about="http://www.somewhere.org/contribution"
<dc:creator>Andrea Rossato</dc:creator>
<dc:title>DRM Systems and Trusted Computing</dc:title>
<dc:subject>Semantic Web</dc:subject>
</rdf:Description>
</rdf:RDF>
```

Legal Semantics

P3P:

- a semantic web approach to describing privacy policy of web sites
- Browser should accept the policy in accordance with user preferences

XrML and MPEG Right Expression Language:

- A way to espress rights and duties over digital resources
- Statements about user rights to:
  - Adapt, Delete, Execute, Install, Play, Uninstall, etc.

Legal Semantics

- Legal Semantics must be enforced within the Application Layer:
  - Applications must comply with legal statements embedded in digital resources
  - Application must be trusted
    - Who trusts what?

Trusted Computing

- Trusted Computing is not a Digital Right Management System
- Trusted Computing is an essential requirement for DRM Systems
  - A way of certifying applications' compliance with legal statements about rights over digital resources
  - A trusted system is a system trusted by copyright holders

Trusted Computing

Trusted Platform Module (aka Fritz's Chip):

- Root of Trust for certifying the OS and Applications that run on top of it
- Must be hardware implemented
- Trusted mode requires the OS and the applications to be digitally signed and certified

Trusted Computing

Trusted Platform Module (aka Fritz's Chip):

- Root of Trust for certifying the OS and Applications that run on top of it
- Must be hardware implemented
- Trusted mode requires the OS and the applications to be digitally signed and certified

Trusted Computing

- Digital Self-help
  - Self-help strictly regulated in the “real” space
  - General prohibition of self-help, unless explicitly permitted
  - Pervasiveness of digtal self-help