NRC·CNRC

Institute for
Information
Technology

Digital Rights Management

Stephen Downes
National Research Council Canada

September 15, 2006

National Research
Council Canada

Conseil national
de recherches Canada

Canada

Overview…

- The New Ethos
- Approaches to DRM
- DRM Doesn’t Work
- Authentication and Identification
- Distributed DRM

The Ethics…

- Is file sharing wrong? We are being told it is, but there is a new (though somewhat underground) ethos at work today…
- Is *sharing* wrong? The Pig and the Box
  http://dustrunners.blogspot.com/2006/07/pig-and-box.html
- Are the publishers in the right? Consider…
- September 19 – Talk Like a Pirate Day
  http://www.talklikeapirate.com/piratehome.html

The Purpose

- The purpose of copyright, of DRM, is to prevent the reuse of materials
- When people lose this power, they feel a real loss
- But it is a fictional loss – this sort of control is a right they never had
- You can't lose the right to control language
- It's not about the money at all, it's about control – we need to understand this up front

The New Ethos

- Copyright, Ethics and Theft
  http://www.downes.ca/cgi-bin/page.cgi?post=65
- Derrida: copying is required for communication – words, icons, images
- The taking of words, images, etc., out of the public domain is theft
- Example, the Blackweb patent case
  http://www.downes.ca/blackboard_patent.htm

Reuse

- Is Reuse Immoral? Would it be immoral to take my stereo back from a thief? http://www.downes.ca/cgi-bin/page.cgi?post=65
- Where do we draw our lines between reuse and theft… "Plagiarism is thievery," writes Christopher Tipton. Well congratulations to Mr. Tipton for having come up with that original idea!

What is DRM

- **Digital** – specific to digital resources, such as electronic documents and media
- **Rights** – concerned with ownership and the terms and conditions of use
- **Management** – concerned with creating mechanisms to enable or prevent use

Aspects of DRM?

- Aspects of DRM
- **Expression** – the description of the resource, ownership of the resource, and the terms and conditions of use
- **Authentication** – verification that the person using the resource has the right to use the resource
- **Protection** – means, such as encryption, to ensure only authorized users have access

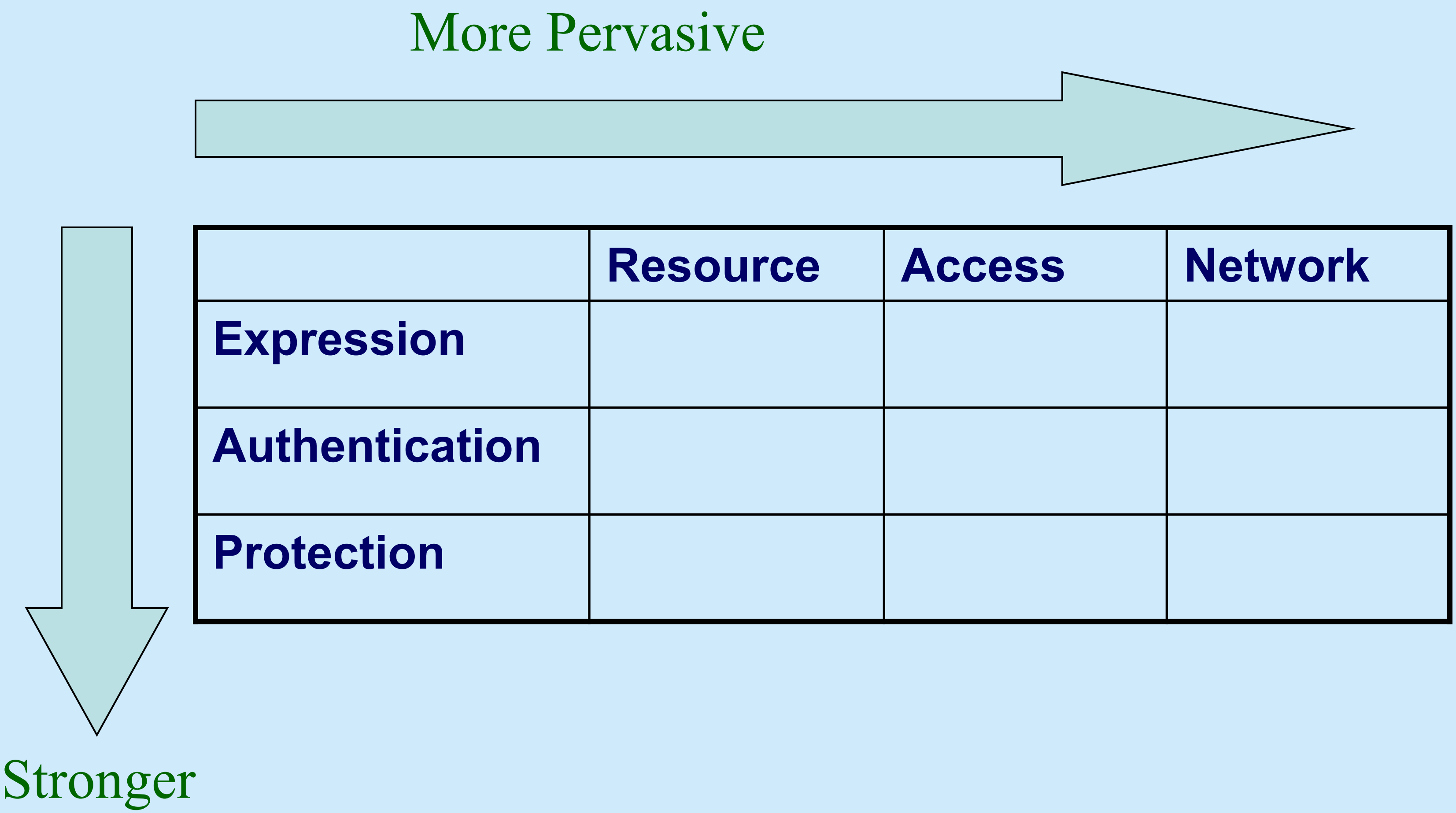
Where DRM is Applied

- Where DRM is Applied
- **Resource** – a particular document or digital resource – for example, a document may be locked or encrypted
- **Access Point** – a content server, such as a website – for example, a website may require a login
- **Network** – the connections between servers – for example, ATM network

DRM Design Decision Metric

	Resource	Access	Network
Expression	Copyright notice	Terms of use notice	Rights expression language
Authentication	Password to open document	Password to access website	PIN to use ATM system
Protection	Encrypted document	Secure sockets layer	Virtual private network (VPN)

Degrees of DRM



More Pervasive

Stronger

	Resource	Access	Network
Expression			
Authentication			
Protection			

Weak DRM

- *Expression:* in the resource only
- *Authentication:* none
- *Protection:* none
- Examples: web page with a copyright notice, book with a copyright page, property with a ‘keep out’ sign

Strong DRM

- *Expression:* in the resource, access point, or network
- *Authentication:* network – single login
- *Protection:* network wide
- Example – the ATM system requires that you provide credentials to use the system, and encrypts all data and communication

Issues in DRM

- *DRM is too weak* – in networks like the web and Napster, expression alone is insufficient to ensure that rights are respected
- *DRM is too strong* – proposed DRM systems require a unique userid (eg., MS Passport) and fully secured network (eg., Rights management server, ‘trusted’ applications), violate privacy, fair use

The Middle Way

- *Expression* – supported at the network level through the use of a rights expression langauge
- *Authentication* – supported at the access level through the use of keys
- *Protection* – supported at the document level with locks or encryption

Critics from Both Sides…

- It’s too strong – advocates of open content fear any DRM system will prevent people from freely sharing content
- It’s too weak – commercial providers want stronger protection, such as authentication at the network level, to prevent file sharing

Responses

- It’s weak enough – to use free resources, rights must be declared, and any further level of authentication and protection is at the discretion of the resource owner
- It’s strong enough – a key system makes it difficult to obtain unauthorized access to content, but leaves it easier to buy content than to steal it

What Causes File Sharing?

- When DRM is too weak – there is no incentive to go through the extra work and cost to pay for content; commercial content is not viable
- When DRM is too strong – free content is not viable, and the transaction cost is too high, so it is easier to look elsewhere for the same content

DRM Principles

- *Open Standards* – the mechanisms for expression, authentication and protection can be used by anyone
- *Open Network* – any agency or entity may provide any of the services provided by the network
- *Open Marketplace* – and agency or entity may buy or sell on the network

Rights Expression

- ***Defined at the Network Level***
  - A rights expression language (REL) is used
  - Current support for ODRL because it does not create a cost – XrML, DRML are options if they are royalty free
  - A mechanism for expressing digital rights expression is supported such that these are available anywhere in the network

DRM Doesn’t Work

- The Darknet and the Future of Content Distribution, a 2002 article by Peter Biddle, Paul England, Marcus Peinado, and Bryan Willman, four employees of Microsoft.
- Main point: DRM can always be circumvented
- http://crypto.stanford.edu/DRM2002/**darknet**5.doc

Authentication and Identification

- Nothing in an identity *claim* prevents it from being a false claim
- But – with some few exceptions – nothing in the *authentication* prevents it from being a false claim either
- In other words – there must be *a reason* to protect one’s own identity
- But in DRM, the only beneficiary is the publisher
- http://www.downes.ca/cgi-bin/page.cgi?post=12

NRC CNRC

Institute for Information Technology

http://www.downes.ca

Science at work for Canada

National Research Council Canada

Conseil national de recherches Canada

Canada