



Take a quick survey of the audience:

How many have a known need for DRM

How many consider DRM protecting CAD important

Overview

- DRM basics
- Data management considerations
- DRM approaches
- Conclusions



I'll cover some of the DRM basics. What is DRM and how does it work.

For those who may not know, Wildfire 4 has DRM security capabilities. Wildfire's DRM is managed by Adobe's LiveCycle Rights Management Enterprise Suite. So I'll also touch on some of the capabilities of LiveCycle Rights Management.

I'll also look at the major items to consider when looking at implementing a DRM solution.

We'll also look at two DRM implementations, a simple and a complex approach and draw some conclusions from their experiences.

DRM Basics



“Any technology used to protect the interests of owners of content and services (such as copyright owners). Typically, authorized recipients or users must acquire a license in order to consume the protected material—files, music, movies—according to the rights or business rules set by the content owner. ”

– Microsoft Security Glossary



Generally speaking, DRM is when content owners control how recipients use digital data.

DRM applied to the engineering discipline differs significantly from DRM in the entertainment industry. In the entertainment industry end users pay for the rights to use, be entertained by, digital media. It is quite rare that an engineer will pay to view a Pro/ENGINEER model to be entertained. Usually, the owner shares the model for some mutual benefit of both owner and recipient.

DRM Basics

- DRM controls the *usage* of the data as opposed to the *access* of the data
 - PLM / PDM / CMS control access
 - DRM controls usage



Digital Rights Management is the definition and enforcement of usage privileges.

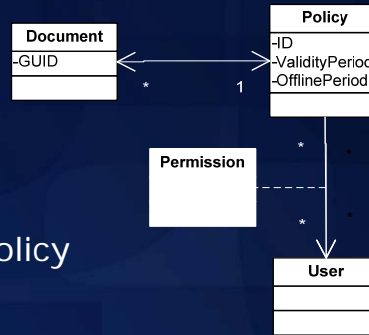
Most controls in existence, today, in engineering, are access control. Access control is managed by PLM, PDM and content management systems. These systems enforce who can download data. Once downloaded there are no more controls in place.

Whether accidental or malicious, once data is downloaded it has the potential to be “leaked” to competitors, to the news media, or a myriad of other unforeseen destinations. These destinations may not be in the best interest of the owner and could, potentially, harm the intellectual property owner. Thus, there is a need for DRM for engineering.

DRM controls the usage of the data. Even after being downloaded, the intellectual property owner can determine who has rights to open, copy, print, or modify the data. The owner can even change those rights after the file has been distributed.

DRM Basics - Logical

- Policy
 - Permissions by groups / users
 - Validity period
 - Expiration date
 - Audit usage
 - Offline access
- Multiple documents per policy
- Multiple users per policy



The DRM basics I'll be showing today are based upon Adobe's LiveCycle Rights Management Enterprise Solution. Wildfire 4 has the capability to secure Pro/E files using Adobe's LiveCycle Rights Management.

The central control mechanism is the Policy. One or more files can be rights managed by a single policy.

Each user, when added to a policy, is given specific usage permissions for all files managed by that policy.

A change to the policy affects all files that are managed by that Policy.

If a policy allows Offline access, the user can, while on-line, synchronize with the server to obtain permission sets for a time period defined by the policy. Then, while within the offline lease period, the user can open and use protected files even if not on-line.

DRM Basics - Physical

- File encryption
 - Each file given unique identifier
- LiveCycle policy server
 - Policies and permissions
 - Authentication of users
 - Key generation and distribution
 - Audit events
- Application (Pro/E, PDF, CATIA V5, Word, Excel)
 - Retrieves keys and permissions from policy server
 - Enforces permissions



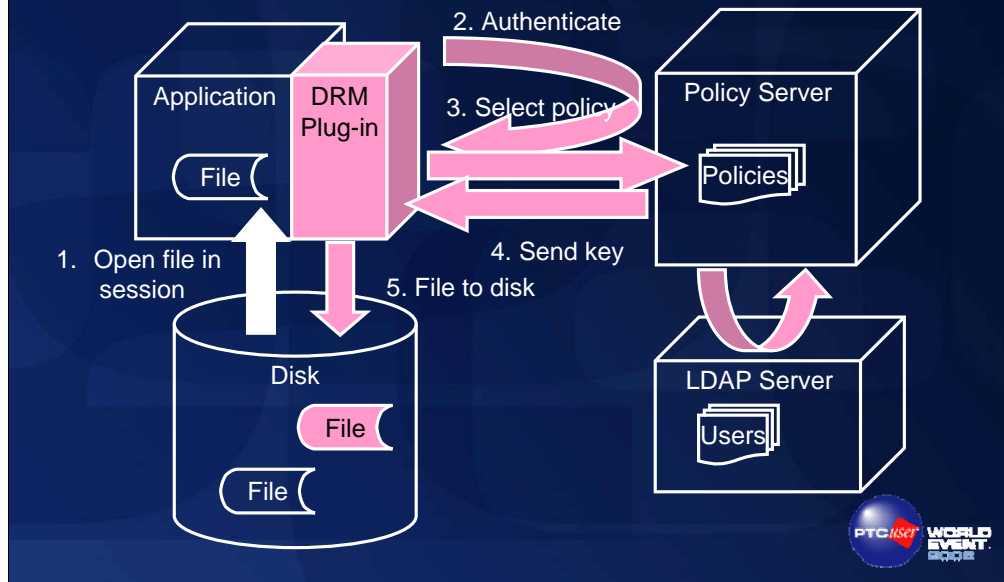
The three physical components are the file, the policy server and the application.

The file when secured is encrypted and is registered with the server with a unique identifier. Only the file identifier is sent to the policy server, the files, themselves, are never sent to the server.

The LiveCycle Rights Management Policy Server manages policies and user permissions on those policies. The Policy Server authenticates users, generates keys used for encryption and decryption, informs applications what permissions a given user has for a given file, and logs activity.

The application requests authentication, retrieves keys and permission sets from the Policy Server, performs the encryption, enforces those permissions.

DRM Secure Use Case

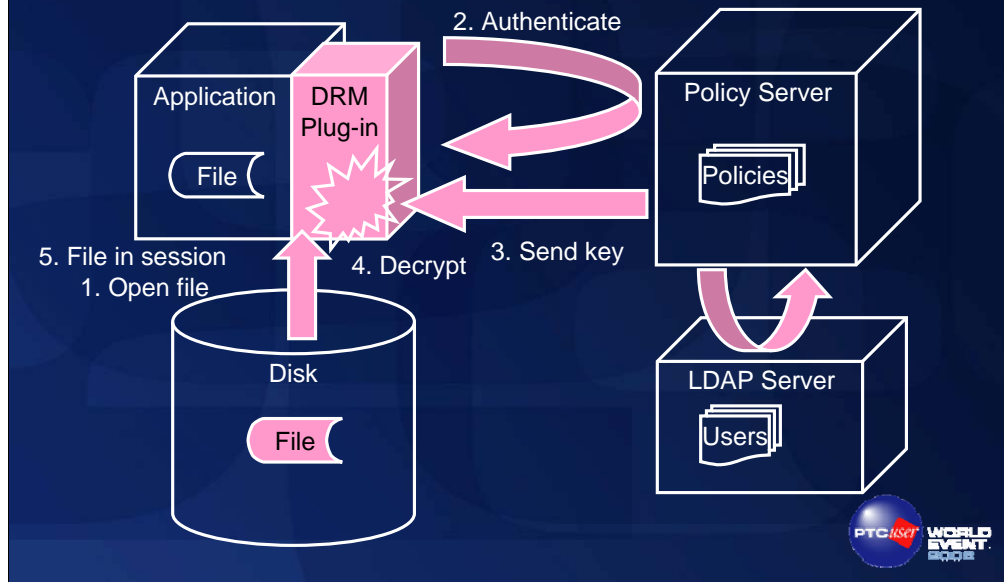


This diagram shows the components of the system. The DRM plug-in shown is integral with some applications such as Wildfire 4.

To secure a file the user:

1. Opens the unprotected file in the application, WF4 for example;
Selects the 'Secure' option;
2. Authenticates with the policy server;
3. Selects the policy that will manage this file;
- 4. The policy server generates a unique identifier and sends the encryption key to the application**
5. The application encrypts and saves the file to disk.

DRM Open Secured Document Use Case



To use a secured file the user:

1. Opens the file as normal, but during the open process the DRM enabled application recognizes the file as being encrypted
2. The user then authenticates with the policy server, unless already authenticated
3. If the user is authorized to open the file, a key is sent to the application
4. The file is decrypted and placed into session

The application would then restrict certain actions depending upon the permissions granted the user by the file owner

DRM Basics – Features

- Persistent protection
 - Regardless of copies
 - Regardless of distribution
- Dynamic control
 - Owner can change permissions anytime
- Offline access
 - Limited period access while offline
 - Configured on policy



A protected file remains protected regardless of how many copies have been made and where those copies may be sent. All copies would have the same file identifier and thus are protected by the same policy.

The owner can make any change to a policy or revoke access to a file at any time. Those changes go into affect immediately and affect all copies of the files involved. The exception to this is if someone is offline and has previously synchronized with the server, the changes will not go into affect until the user is online or if the offline lease period expires the user will not have any usage rights.

Data Management Considerations



Security Versus Collaboration

- Collaboration and security are opposite objectives
- Both must be considered in tandem
- Security officer
 - Protect everything to the nth degree
- Engineer
 - Keep everything wide open
- Find a balance between security and collaboration



When considering a rights management strategy the dilemma you face is finding the appropriate balance between security and collaboration.

Typically, the Information Security Officer wants to lock down everything, protect all IP, and only open up what is necessary.

On the other hand, the Engineering Manager wants everything open and available, locking down only what is necessary to be protected.

The balance you choose will affect how you organize your data and the amount of resources required to manage the system.

Policy Considerations

- Create policies by
 - Company (least flexible – least cost)
 - Department
 - Product
 - Project
 - File (most flexible – highest cost)
- Windchill
 - Project
 - Product / library
 - Domain



Organize your documents based upon how you want to manage them, by product, department, project...

You would typically have 1 DRM policy for each document group. Or you may have a small set of policies for 1 document group, where each policy manages a different lifecycle state for that group of documents.

The fewer document groups you have the easier it is to manage but you will have less flexibility. If you want maximum flexibility you can assign a different policy for each document. Very flexible but costly to manage.

Consider the structure of your PLM system. By aligning your DRM policies with your PLM structure you may gain some economies of scale. By this I mean some of your rights management tasks could be automated into your PLM management tasks.

User Considerations

- Group users by
 - Company (least flexible – least cost)
 - Department
 - Role
 - Individual (most flexible – highest cost)
- Windchill
 - Internal users
 - External users



Next you will group your users. Again you are balancing flexibility with cost. Consider both your internal and external users.

Finally, I would compare the DRM usage strategy with the PLM access strategy. If they are not somewhat in line I would review them to determine if they will meet the business objects, that balance between security and collaboration.

Apply Permissions

- Determine permissions
 - For each user group
 - For each policy
- Determine off line periods for each policy
- Windchill
 - Policy permissions reflect ACLs



Once the users are grouped and policies defined, you will associate users (groups) to the policies and set permissions for each. Permissions include Offline, Change, Copy and Print.

The permissions should “reflect” the Access Control Lists you’ve defined in Windchill.

Authentication Considerations

- Weak
 - Name
 - Password
- Strong
 - Certificates
 - Biometrics



Another area to consider is the strength of authentication. Both Windchill and LiveCycle Policy Server can use the LDAP server for authentication.

Additional security measures can be added including certificates and even biometrics. Each additional authentication mechanism provides greater security but adds management cost.

Process Considerations

- Quantity of documents
- Frequency and type of changes
- Ownership of documents
- Define processes
 - Manual vs. automatic
 - Individual vs. batch
- Windchill
 - Event triggers
 - Manual control



Your business processes must also be considered.

How many documents will be protected?

At what frequency will new documents or new versions of documents be secured?

Who will be the owner of record of the secured documents?

Will documents be secured manually or automatically as part of a workflow?

Data Flow Considerations

- Master documents
 - Secured
 - Unsecured
- Distribution - internal vs. external usage
- Windchill
 - WTDocuments
 - Secondary content
 - External network shares



You will also want to review your data flow.

Many decide to keep the master version unencrypted in a secure location, Windchill perhaps.

Currently, a secured Wildfire file cannot be uploaded or checked into Windchill. But you may want to download your Wildfire files, protect them, and put them onto a shared drive so they can be distributed externally.

DRM Approaches



Now we will look at two rights management approaches. Two companies, A and B.

Company A

- North American manufacturer with dozens of sites
- Content management system
 - SharePoint
- Need
 - Protect documents related to specific transaction sets
 - Each transaction has multiple documents
 - Each transaction set shared with different external partners



Company A is a manufacturer/supplier with many sites in North America. Company A uses Microsoft's SharePoint as its content management system.

Company A has sets of documents that are relevant to particular transactions. The group of people who need access to the documents are consistent across each activity, but differ between transactions.

Company A - Simple Approach

- Group documents by transaction set
 - Each set in its own library
- Group users by partner company
- One policy for each transaction set

- Each document saved in a “protected” library
 - Automatically gets protected
- Users added or removed from library are manually added or removed from policy



Company A's strategy is to group documents by transaction. The documents for each transaction are stored in its own library in the content management system. Users are grouped by their company affiliation. There is one policy per library (transaction).

Company A is creating an automated process where a file, in this case a PDF file, protected when it is saved into a library. The secured file is associated to the policy defined for that library.

Users are added manually to both the content management system and the rights management server. As these groups are relatively small and do not change frequently, this is sufficient.

Company A - Status

- Planning stage
- Time to implement - weeks



Company A is currently in the planning stage.

Implementation time is in weeks, that is less than a month.

Company B

- European manufacturer
- Content management system
 - Home grown
- Need
 - Upcoming manufacturing joint venture with China
 - Protect new feature designs
 - Protect only when outside trusted environment



Company B is a European manufacturer. It has a home-grown content management system.

Company B is engaging in a joint venture in China. It needs to protect the new features of its designs. Only those files that are being distributed outside of its trusted environment need to be secured.

Company B - Complex Approach

- Group documents by individual file
- Group users by department
- One policy per file

- Each document staged for distribution gets protected
- Requires set of administration tools
 - Create policies
 - Revoke access to old revisions
 - Add / remove users



Company B wants flexibility. Company B has decided to create one policy for each file. The users will be grouped by department.

As a document is staged for distribution it will be protected.

In order to have this level of flexibility, Company B is planning a set of tools to automate many of the administration tasks required to manage the system.

Company B - Status

- On hold
- Time to implement - months



Company B's project is not yet implemented.

Time to implement is months.

Conclusions



Conclusions

- Identify your threats
- Determine a DRM path
- Balance security and collaboration
- Start small – a little DRM is more protection than what you have now
- Use Windchill for **access control** and DRM for **usage control**
- Minimize management duplication between Windchill and policy server



Identify your threats

Determine your rights management path

Balance security against collaboration (openness)

I think the most important thing is to start simple, start small. A little protection is probably more than you have now

Remember Windchill controls access and rights management controls usage

Determine ways to minimize management, look for ways to gain an economy of scale between your security systems

