DRM Overview

4th Annual IT Security
Automation Conference
NIST Gaithersburg, MD

John T. Landwehr, CISSP
Director,
Security Solutions & Strategy
Adobe Systems Incorporated

September 24, 2008

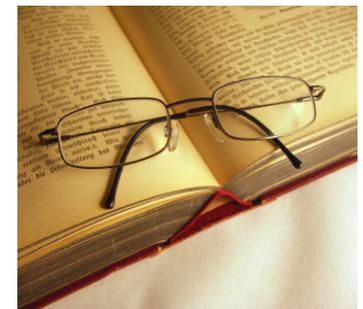# Hollywood DRM vs. Government DRM

Studio Content
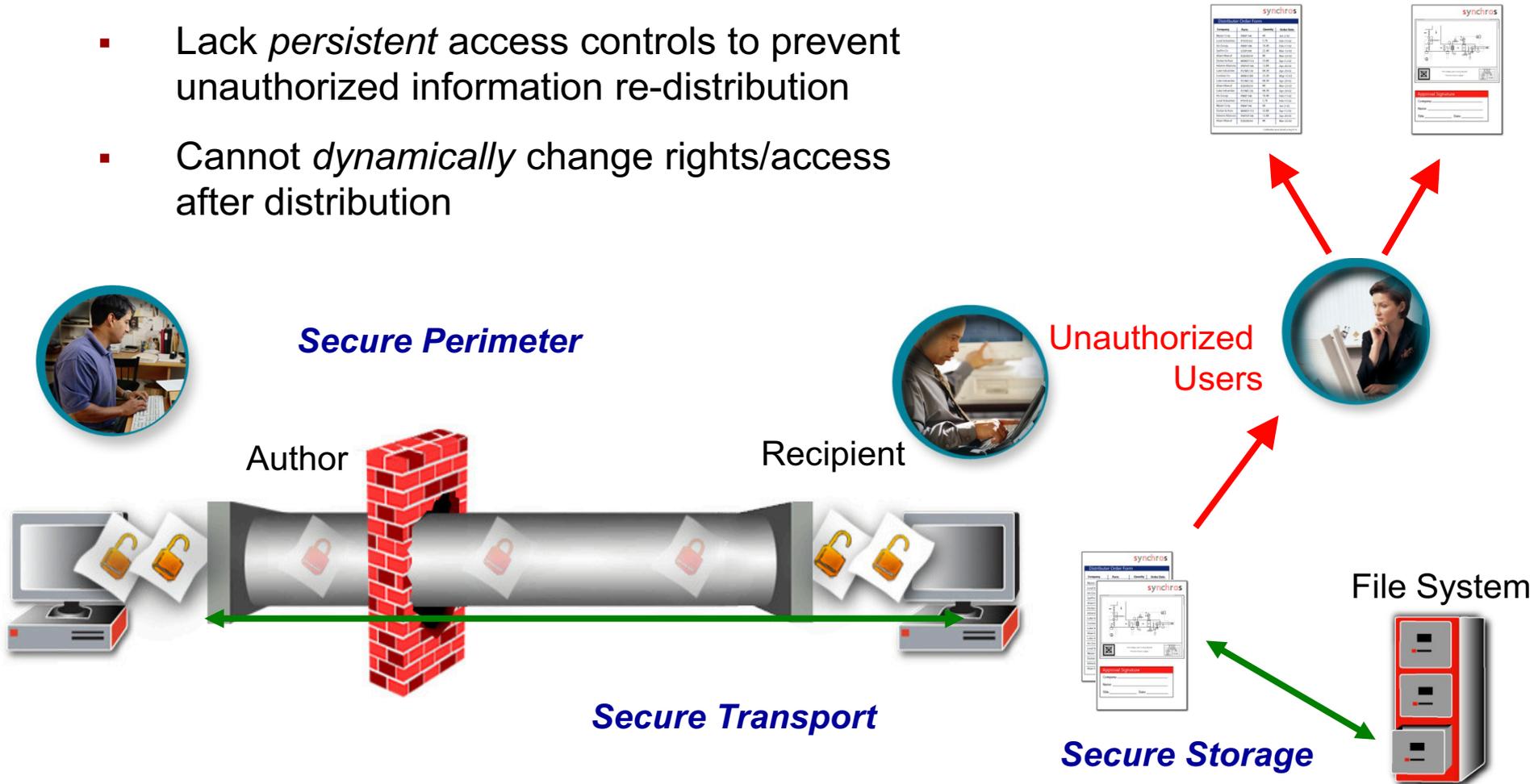

Hackers   **Espionage**   **Secrets**   **Privacy**   **Regulation**

Government Content

Adobe

Issues For Many Information Assurance Approaches

- Lack *persistent* access controls to prevent unauthorized information re-distribution

- Cannot *dynamically* change rights/access after distribution

Secure Perimeter

Author

Recipient

Unauthorized Users

Secure Transport

File System

Secure Storage

Protection must consistently persist in multiple native formats

Rights Management Can Facilitate:

- More secure sharing

- Key management

- Automation of protection

- Auditing

- Security persistence

Independent of storage and transport

DRM: 1ˢᵗ Generation

- Not really DRM.

- Sensitive content is wrapped in a container file type (e.g. zip, pgp)

- That file is encrypted with a password in that external application

- Recipient types in password, unencrypted and unprotected files are removed

Once decrypted, unprotected content can be accidentally or maliciously redistributed

- Native file is encrypted in native application

- RC4/AES encryption based on a shared password

- Permissions disable print, modify, clipboard

- Those permissions are the same for all recipients

- Recipient receives file, enters password, interacts with protected content

Shared passwords aren't secure enough

- Native file is encrypted in native application

- RC4/AES encryption using PKI and directory

- Permissions disable print, modify, clipboard

- Each addressed recipient may have different permissions associated with their public key

- Recipient receives file, decrypts w/ private key, interacts with protected content with their individualized permissions

Limited permissions aren't mapped to a cross-application policy and cannot be dynamically managed inside/outside an organization

DRM: 4th Generation

- Native file is encrypted in native application

- AES encryption managed through webservices to a rights management server

- Server is connected to internal and external directories of users and groups

- Server maintains list of policies that map users and groups to permissions

- Sender or automated process specifies policy by name to encrypt

- Recipient authenticates to rights management server to decrypt file and interact with the protected content based on the policy permissions

- Recipient actions can be audited

Today's Rights Management features

- Directories:
    - LDAP
    - AD (including DL- and ORG- Exchange mailing lists)
    - Custom
- Permissions:
    - Open
    - Print
    - Modify
    - Clipboard
- Additional controls:
    - Expiration (absolute, relative, immediate revocation)
    - Version Control
    - Change policy on existing documents
    - Watermarking
    - Online/Offline
    - Auditing
- Ad-hoc and structured processes
    - User initiated on desktop
    - Mapped to ECM/PLM system
    - Built into workflow process

Sample Policy Management

Applying DRM to applications on the desktop
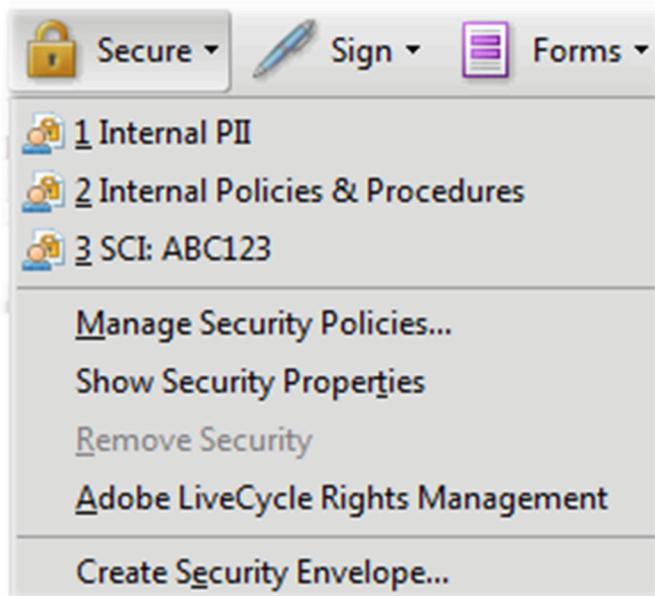
Two clicks to apply policy

Those policies can be
• Organization-wide
• Workgroup
• Personal

Apply DRM in an Automated Process
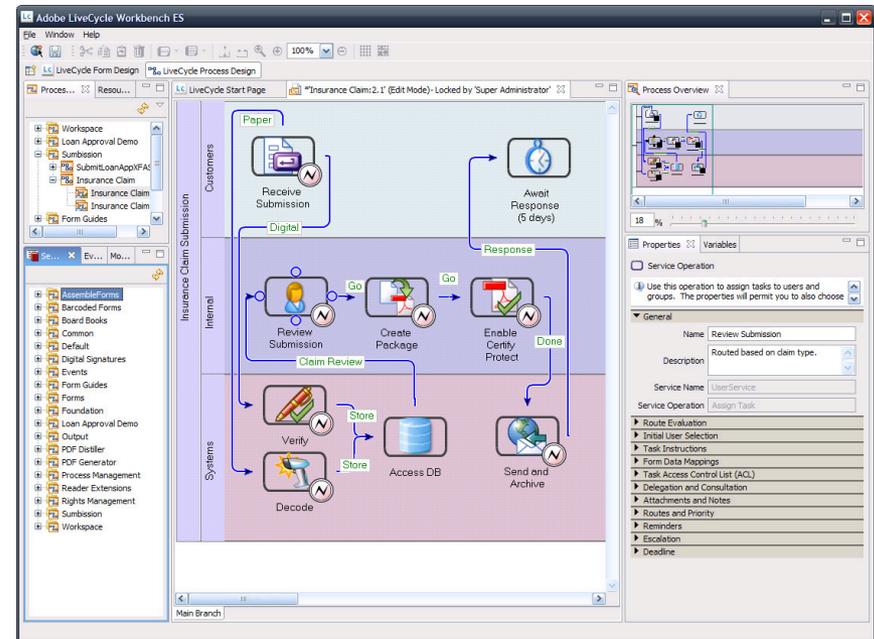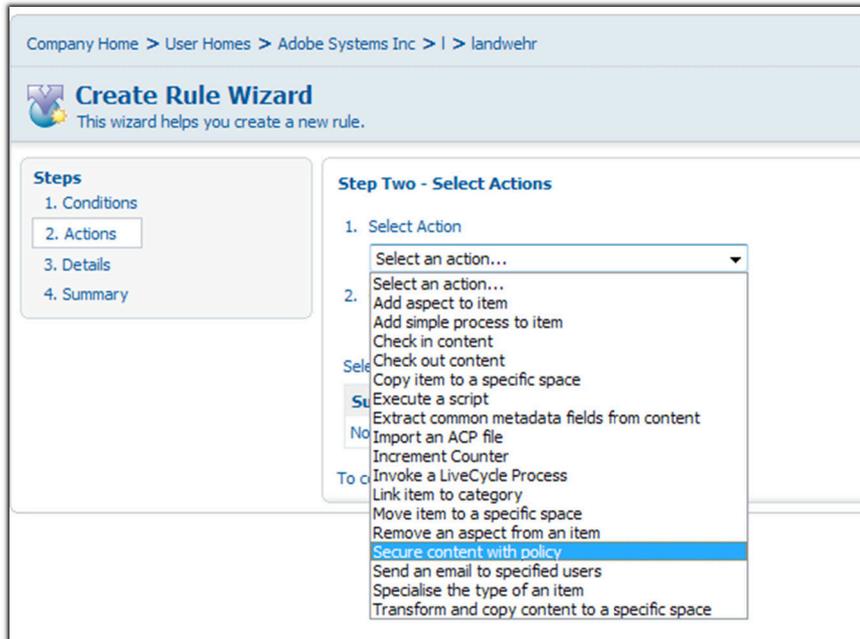
Policies can be applied through content management systems and electronic document workflows

In DRM: Authentication is tied to document opening
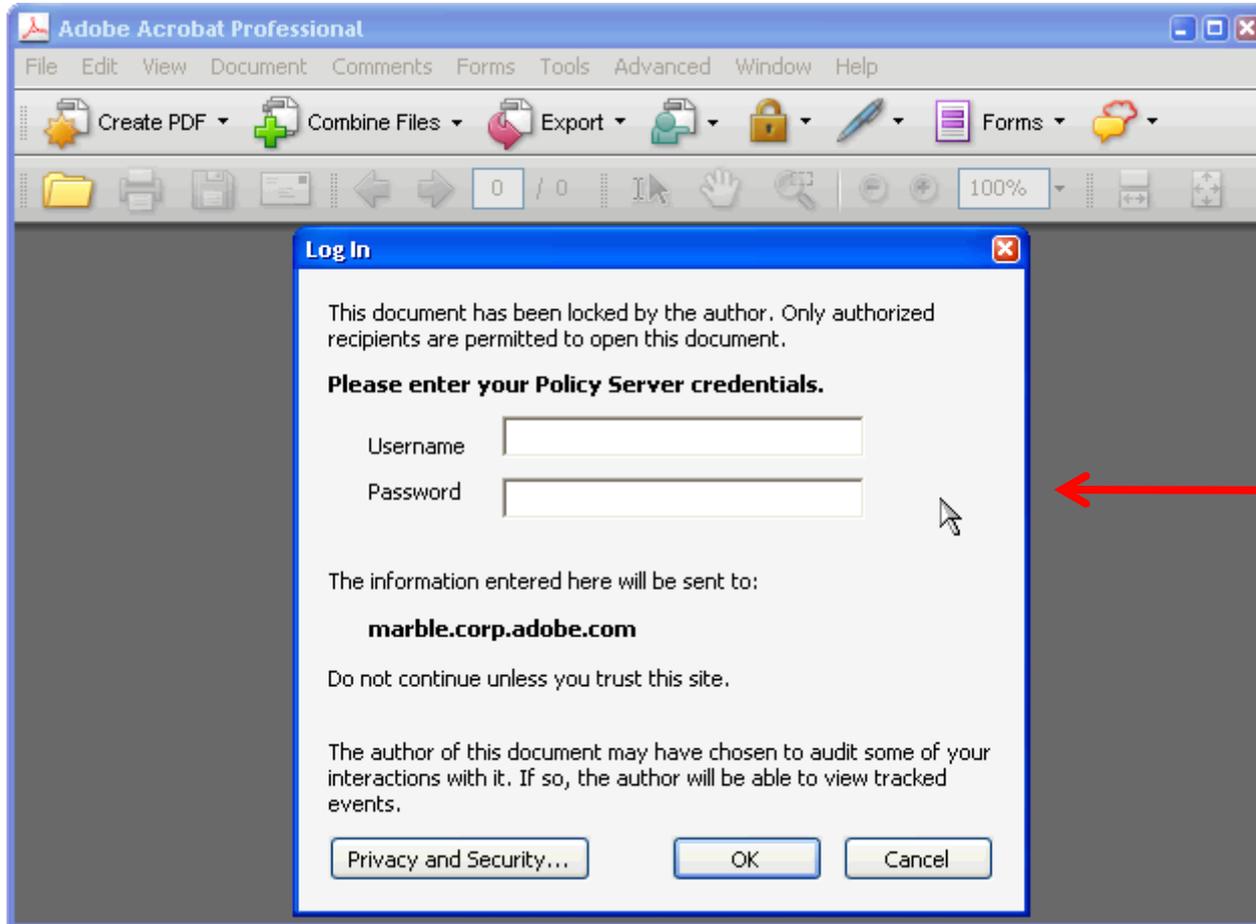
Common authentication options:

- Username+password
- Username+OTP
- Kerberos SSO
- PIV/CAC PKI

DRM Preventative Control Permission Enforcement
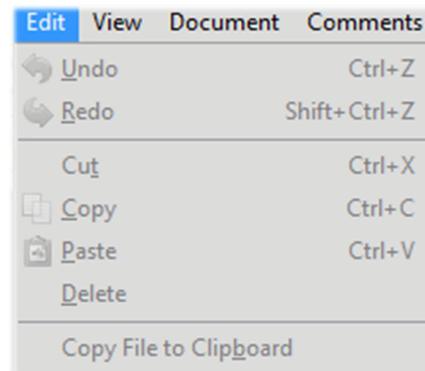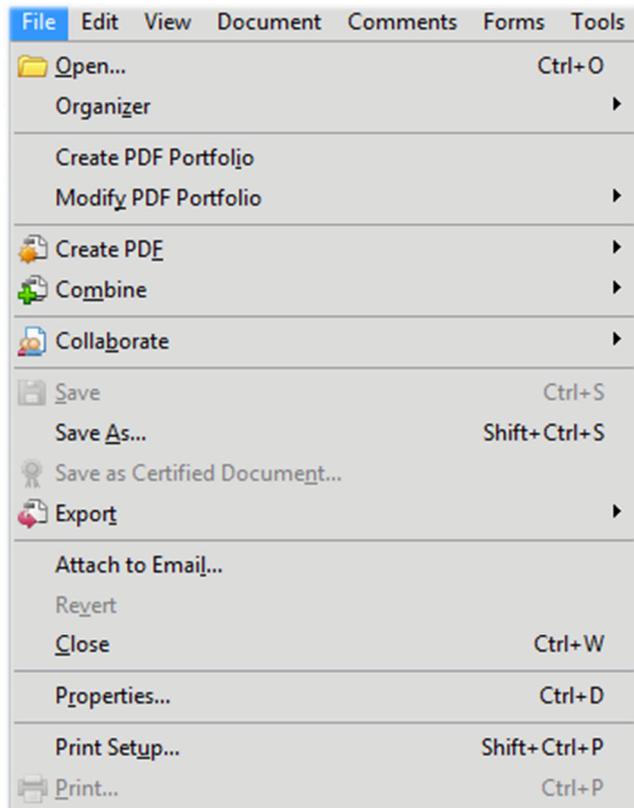
DRM Protecting native formats

DRM protecting CAD files

Video DRM

Not just for consumers watching movies and TV shows from the studios.

Policy protection for:
- Recorded meetings
- Online training
- Surveillance footage

Detective Controls through Dynamic Watermarking

More watermark options

Really Obvious

Very Subtle

DRM Summary

- Right management is content-centric security on native formats

  - documents, forms, media

- Protects information throughout its lifecycle

  - create -> collaborate -> archive -> destroy

- Maintains protection inside and across organizations

- Persistent protection

  - independent of storage and transport; online & offline

- Applied via ad-hoc and structured processes

- Only the intended recipients can interact with protected content

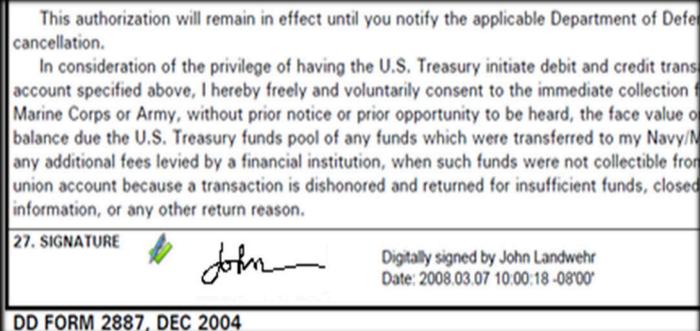# Adobe Initiatives Of Interest to Government

LiveCycle Rights Management

Acrobat and Reader JITC Certification

FIPS 140-2 modules AES256 & SHA512 FDCC

Certified Documents

Digital Signatures

Redaction & Sanitization

CAC & PIV Support

For more information:
http://adobe.com/government
http://blogs.adobe.com/security
John Landwehr: (408)536-6763; jlandwehr @ adobe

Adobe