Digital Right Management

(Gestión de Derechos Digitales)

Quiong Liu, Reihaneh Safavi-Naini y Nicholas Paul Shepppard

School of Informatics Technology and Computer Science
University of Wollongong
Australia

Paper presentado en el Workshop *AISW2003* (*Australasian Information Security Workshop 2003*)

Cronograma

*** Descripción General de los Sistemas DRM**
*** Utilización de DRM en los sistemas comerciales actuales**
*** Análisis de las medidas de seguridad**
*** Inquietudes de los consumidores**
*** Estandarización de DRM**
*** Factores de éxito - Conclusiones**

Descripción General de los sistemas DRM

Definición : "Sistema para proteger contenido digital y para controlar la distribución y uso de dichos contenidos."

En la actualidad, se puede utilizar Internet para distribuir música digital, imágenes, videos, libros, juegos, etc.

Para proteger la propiedad intelectual digital comercial y evitar la piratería digital, se necesita un sistema que prevenga accesos no autorizados y que administre los derechos de uso de los contenidos digitales.

Descripción General de los sistemas DRM (cont)

Un sistema DRM debe:

administrar los derechos de uso de los diferentes tipos de contenidos digitales a través de diferentes plataformas (PC´s, laptops, PDA´s, teléfonos móviles, etc) y controlar el acceso al contenido distribuído sobre diferentes tipos de medios físicos (CD-ROM´s, DVD´s, flash memory, etc)

Descripción General de los sistemas DRM (cont)

Licencias Digitales
Son archivos de datos que especifican ciertas reglas de uso sobre un determinado contenido digital

- **El usuario compra una licencia que le concede ciertos derechos de uso.**
- **Reglas de uso : frecuencia de accesos, tiempo límite de uso, restricciones de transferir a otros dispositivos, permisos para copiar, etc.**
- **Modelos Comerciales : alquiler, subscripción, try-before-buy, pay-per-use, etc.**

Descripción General de los sistemas DRM (cont)

El modelo DRM

- DRM debe estar integrado con un sistema de e-commerce que administre todo el mecanismo de pagos financieros
- Existen diferentes implementaciones de DRM
- El proceso es básicamente el mismo y participan 4 actores

Descripción General de los sistemas DRM (cont)

- **Proveedor : mantiene los derechos digitales sobre los contenidos y desea proteger esos derechos (ej: productora de música o un estudio de películas)**
- **Distribuidor : provee los canales de distribución, como ser un sitio web para compras on-line**
- **Consumidor : utiliza el sistema descargando los contenidos digitales y paga por las licencias para su uso**
- **Casa de cambio (clearinghouse) : administra las transacciones financieras para entregar las licencias a los usuarios y para pagar las correspondientes ganancias a los proveedores y distribuidores**

Descripción General de los sistemas DRM (cont)

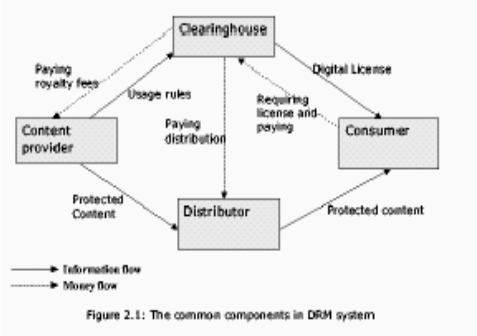

Figure 2.1: The common components in DRM system

Descripción General de los sistemas DRM (cont)

Un usuario puede obtener un contenido y re-distribuirlo libremente a otros potenciales usuarios, pero cada uno de ellos tendrá que adquirir sus propias licencias para poder utilizarlo.

Otras variantes:

Las licencias pueden ser distribuídas a las aplicaciones antes, o en el mismo momento que se transfiera el contenido protegido (para licencias temporales con propósitos promocionales "try-before-buy")

Descripción General de los sistemas DRM (cont)

Plug-ins

Las aplicaciones del cliente (reproductores de música o video, visualisadores, etc) son las encargadas de desencriptar los archivos protegidos adquiridos en un sistema DRM.

No existe interoperabilidad entre los distintos sistemas DRM. Cada sistema requiere su propio plug-in.

Cronograma

* Descripción General de los Sistemas DRM
* **Utilización de DRM en los sistemas comerciales actuales**
* Análisis de las medidas de seguridad
* Implicaciones legales
* Inquietudes de los consumidores
* Estandarización de DRM
* Factores de éxito

Utilización de DRM en los sistemas comerciales actuales

Microsoft WMRM

- **Para distribución de archivos multimediales.**
- **Basado en Windows Media Player. Soporta solamente formatos WMA (Windows Media Audio) y WMV (Windows Media Video).**
- **Modelos comerciales: subscripción, venta, operaciones contadas, transferencias seguras de contenidos multimediales hacia dispositivos portables.**
- **Principal ventaja: los formatos de Windows están ampliamente difundidos en Internet.**

Utilización de DRM en los sistemas comerciales actuales (cont)

InterTrust Rights|System

- **"pay-per-use", rentals, ventas, "try-before-buy".**
- **PC´s de escritorio, teléfonos móviles, set-top boxes, y ciertos reproductores musicales.**
- **Adobe Acrobat para leer/editar documentos, MusicMatch, reproductores MPEG-4.**
- **Nokia utiliza InterTrust para distribución de contenido móvil.**

Utilización de DRM en los sistemas comerciales actuales (cont)

IBM EMMS

- **Desarrollado para clientes IBM.**
- **"pay-per-use", "pay-per-time", subscripción, impresión controlada, transferencia protegida a dispositivos portables.**
- **Sony lo utiliza para distribución de contenido de dispositivos móviles.**

RealNetworks RMCS

- **Para Windows y UNIX.**
- **Subscripción, video por demanda y otros modelos menos conocidos.**
- **Utilizado por MusicNet, AOL Time Warner, EMI Group.**

Utilización de DRM en los sistemas comerciales actuales (cont)

Otros proveedores DRM :

- Adobe,
- Liquid Audio,
- Alchemedia,
- ContentGuard,
- Digital World Services,
- SealedMedia,
- etc

Utilización de DRM en los sistemas comerciales actuales (cont)

Mercados potenciales para aplicar DRM

• e-health. Almacenar y transferir información médica de pacientes a través de redes públicas abiertas.

• e-learning. Intercambiar trabajos de investigación entre instituciones (libre o pago).

• intercambio de documentos dentro de una intranet coorporativa

Cronograma

* Descripción General de los Sistemas DRM
* Utilización de DRM en los sistemas comerciales actuales
* **Análisis de las medidas de seguridad**
* Inquietudes de los consumidores
* Estandarización de DRM
* Factores de éxito - Conclusiones

Medidas de Seguridad

El nivel de seguridad requerido va más allá de otorgar solamente licencias a usuarios autorizados.

Un sistema DRM requiere protección de contenido en forma persistente.

Las restricciones en el uso de ese contenido deben permanecer luego de que el producto haya sido entregado al usuario final.

Medidas de Seguridad

Elementos esenciales de seguridad:

- protección de los datos, para evitar la modificación no autorizada
- identificación única del receptor, para permitir su acceso al contenido adquirido
- mecanismo efectivo para procesar los datos protegidos y reforzar los derechos de uso sobre ese contenido.

Medidas de Seguridad - Modelo de confianza

Modelo de Confianza

No es suficiente solamente con aplicar un modelo de encripción.

Internet provee canales de distribución abierta para consumidores finales que desean intercambiar sus contenidos digitales con sus amigos.

En el modelo de seguridad de DRM no es posible distinguir usuarios honesto y deshonestos.

Medidas de Seguridad - Modelo de confianza (cont)

Ciertos usuarios maliciosos (crackers) pueden llegar a romper el sistema de seguridad para obtener beneficio económico y/o revelar en Internet el modo de hacerlo, incentivando a generar nuevos atacantes.

Medidas de Seguridad - Mecanismos criptográficos

Mecanismos Criptográficos

Encripción simétrica : El contenido digital se encripta/desencripta mediante un algoritmo que utiliza la misma clave (secreta).

Alternativas: algoritmos confidenciales vs. algoritmos "bien conocidos" (ej: AES Advanced Encryption Standard)

Medidas de Seguridad - Mecanismos criptográficos (cont)

Encripción asimétrica : La encripción/desencripción se basa en el uso de pares de claves que están matemáticamente relacionadas. El contenido encriptado con una clave (pública) solamente puede ser desencriptado con la otra clave (privada).

Firmas digitales : Se utilizan para reforzar el aspecto de no-repudio. La casa de cambio (clearinghouse) debe firmar las licencias que entrega. El usuario tiene la firma como constancia de las licencias compradas.

Medidas de Seguridad - Mecanismos criptográficos (cont)

Funciones Hash "one-way" : Se utilizan combinadas con las firmas digitales para el chequeo de integridad del contenido.

Certificados Digitales : Se utilizan para autenticar o verificar la identidad de las partes involucradas del sistema.

Medidas de Seguridad - Individualización

Individualización

Cada licencia está asociada a un único dispositivo, de modo que las licencias adquiridas no puedan ser compartidas o reutilizadas en otros equipos.

Esto reduce notablemente el daño causado por los crackers.

Problema de portabilidad. Solución: backup y restauración limitada

Medidas de Seguridad - Watermarks

Marcas de Agua Digitales

Son señales digitales imperceptibles que pueden ser insertadas dentro del contenido con varios propósitos.

Deben recuperarse con software especial diseñado especialmente para leer marcas de agua.

La tecnología actual para embeber marcas de agua dentro de contenido todavía no resulta del todo robusta. Es vulnerable a ataques y fraudes

Medidas de Seguridad - Watermarks (cont)

Usos de las marcas de agua :

• registrar copyright, dueño del contenido, comprador, información sobre el pago, etc.

• rastrear piratas digitales, por medio de web-spiders, con el objetivo de detectar violaciones de copyright.

• "annotation watermarks": asentar datos y controlar el acceso (cantidad de copias permitidas, cantidad de veces que puede reproducirse un tema musical).

• modelos "try-before-buy": acceder a contenido de inferior calidad para evaluarlo, y si está conforme, puede pagar para obtener la versión de óptima calidad.

Cronograma

* Descripción General de los Sistemas DRM
* Utilización de DRM en los sistemas comerciales actuales
* Análisis de las medidas de seguridad
* **Inquietudes de los consumidores**
* Estandarización de DRM
* Factores de éxito - Conclusiones

Inquietudes de los consumidores

Privacidad y anonimidad

El proceso de autenticación requiere que el usuario revele su identidad para acceder a contenido protegido.

Se asigna un identificador único a la aplicación del usuario (reproductor, visualizador, etc) y toda la información personal del usuario se vincula a ese identificador.

Un buen sistema DRM debe proteger la privacidad de los usuarios y permitir accesos anónimos a los contenidos digitales. El sistema no debe generar un vínculo entre la identidad del usuario y sus compras.

Inquietudes de los consumidores

Facilidad de uso

Las implementaciones actuales de DRM presentan algunos inconvenientes de uso :

* **incompatibilidad entre diferentes implementaciones.**
* **cada sistema DRM tiene sus propios plug-ins para instalar sobre las aplicaciones del usuario.**

Cronograma

* Descripción General de los Sistemas DRM
* Utilización de DRM en los sistemas comerciales actuales
* Análisis de las medidas de seguridad
* Inquietudes de los consumidores

*** Estandarización de DRM**

* Factores de éxito - Conclusiones

Estandares

Los problemas de incompatibilidad surgen precisamente por el desarrollo de mecanismos de protección propietarios, no estandarizados.

Varias organizaciones están trabajando hacia la definición de estandares:

- **Open Digital Rights Language Initiative (odrl.net),**
- **World Wide Consortium (www.w3c.org),**
- **Open eBook Forum (openebook.org),**
- **Secure Digital Music Initiative (www.sdmi.org),**
- **Internet Digital Rights Management (idrm.org),**
- **etc**

Cronograma

* Descripción General de los Sistemas DRM
* Utilización de DRM en los sistemas comerciales actuales
* Análisis de las medidas de seguridad
* Inquietudes de los consumidores
* Estandarización de DRM

*** Factores de éxito - Conclusiones**

Conclusiones

DRM es un nuevo concepto multi-facético.

Está aún en una etapa todavía poco avanzada de desarrollo.

Ha cautivado la atención de muchas compañías multimediales y se ha implantado discusiones respecto a su futuro.

Promete ser una alternativa muy buena para aquellos proveedores de contenidos digitales que desean desarrollar nuevos servicios.

Conclusiones

El éxito no depende solamente de los mecanismos de seguridad. La pregunta esencial es :¿El consumidor está dispuesto a aceptar las reglas de juego?.

La industria necesita inventar un modelo de negocios atractivo que sea fácil de usar, a precios razonables y que respete los derechos de los consumidores.

La intervención del Gobierno en la modificación de las leyes también es importante para prevenir la distribución ilegal en gran escala. Un buen ejemplo de esto fue la decisión de la Corte en cerrar el Napster.

FIN

¿ P R E G U N T A S ?