DRM-Systeme

Kai Schmitz-Hofbauer

ITS-Seminar

12.02.2004

Prof. Dr.-Ing. Christof Paar
Lehrstuhl für Kommunikationssicherheit
Ruhr-Universität Bochum
www.crypto.rub.de

Inhalt

- Einleitung
- Mögliche Komponenten von DRM-Systemen
- Beispiele für DRM-Systeme
  - Windows Media RightsManager
  - Intertrust Rights|System
  - Weitere DRM-Lösungen
- Schwächen von DRM-Schutzmechanismen
- Fazit

Einleitung

- **Motivation:**
  - **Firmen wollen den elektronischen Vertrieb für digitale Güter (eBooks, Musik etc.) nutzen**
  - **zugleich aber die illegale Verbreitung durch Raubkopien verhindern**
- **Sämtliche zu diesem Zweck eingesetzten Schutzmechanismen werden von den Anbietern digitaler Güter als DRM bezeichnet**
- ***DRM = Digital Rights Management***
- **Hauptaufgabe: Nutzungsbedingungen des Anbieters bzw. des Rechteinhabers durchzusetzen**

Einleitung

- Festlegung der Nutzungsbeschränkungen, unter denen Kunden digitale Güter nutzen dürfen
  - wer ein Dokument öffnen/ abspielen darf
  - in welchem Zeitraum und wie oft es geöffnet werden darf
  - ob es geändert oder kopiert werden darf
  - die Hardwarekonfiguration, auf der ein digitales Gut genutzt werden darf
  - …
- Kritiker: DRM = *Digital Restrictions Management*

Mögliche Komponenten von DRM-Systemen

- Benutzeridentifizierung
- Verschlüsselung
- Zugriffsschutz
- Authentizität und Integrität
- Kopiersperre
- digitale Wasserzeichen
- Suchsysteme
- Manipulationssichere Hard- und Software
- E-Commerce-Systeme
- Abrechungs- und Zahlungssysteme

Der Windows Media Rights Manager

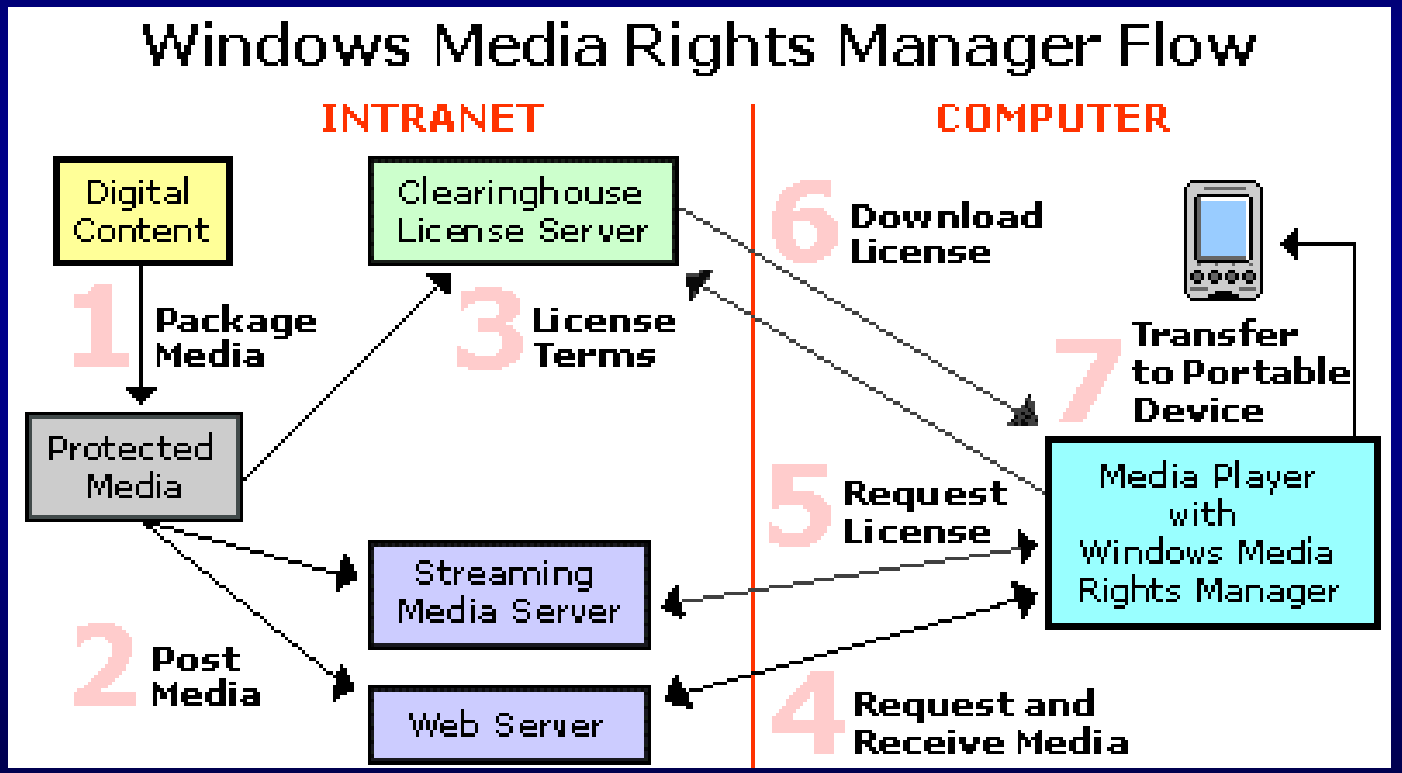
- DRM-Plattform von Microsoft für die sichere Distribution und Nutzung digitaler Inhalte
- ist bereits in die aktuellen MS-Betriebs-systeme integriert
- MS Mediaplayer nutzt ebenfalls diese Technologie
- hat auf Grund des hohen Verbreitungs-grades große Bedeutung
- Typische Einsatzgebiete
  - Musikportale
  - Online-Videotheken

Der Windows Media Rights Manager

- Kein eigenes „Programm“ mit direkter Benutzer-Interaktion, sondern eine Sammlung von COM-Komponenten
- Verschlüsselungskomponente gestattet nur autorisierten Benutzern Zugang zu den Medieninhalten
- Zur Nutzung der Medien wird eine Lizenz benötigt, die unabhängig von den Medien vertrieben wird
- Lizenz enthält den Schlüssel, mit dem verschlüsselte Mediendaten entschlüsselt werden können

Der Windows Media Rights Manager

- Schutz und Vertrieb digitaler Inhalte mit dem Windows Media Rights Manager



- Dateiformate: Windows Media Audio (WMA) und Windows Media Video (WMV)

Der Windows Media Rights Manager

- **Typische Lizenzen beim WMRM**
  - wie oft eine Datei abgespielt werden kann
  - auf welche Abspielgeräte eine Mediendatei übertragen und abgespielt werden darf
  - in welchem Zeitraum die Datei abgespielt werden darf (zum Beispiel Startzeitpunkt und Ablaufdatum)
  - ob und wie oft ein Werk auf eine CD gebrannt werden darf
  - ob und wie oft der Benutzer Lizenzen sichern und wieder herstellen darf
  - auf dem Client benötigte *security level*, um die Datei abspielen zu dürfen

Der Windows Media Rights Manager

- **Anwendungsbeispiel : das Musikportal Musicload (www.musicload.de)**

Intertrust Rights|System

- DRM-System zum Schutz jeglicher Art von digitalen Gütern
- Einsatz von offenen Standards wie XML und Java → integrierbar in andere Anwendungen
- Nicht kompatibel zum Media Player
- Vier Produktlinien
  - Packager
  - Server
  - Clients
  - Software Development Kit (SDK)

Intertrust Rights|System

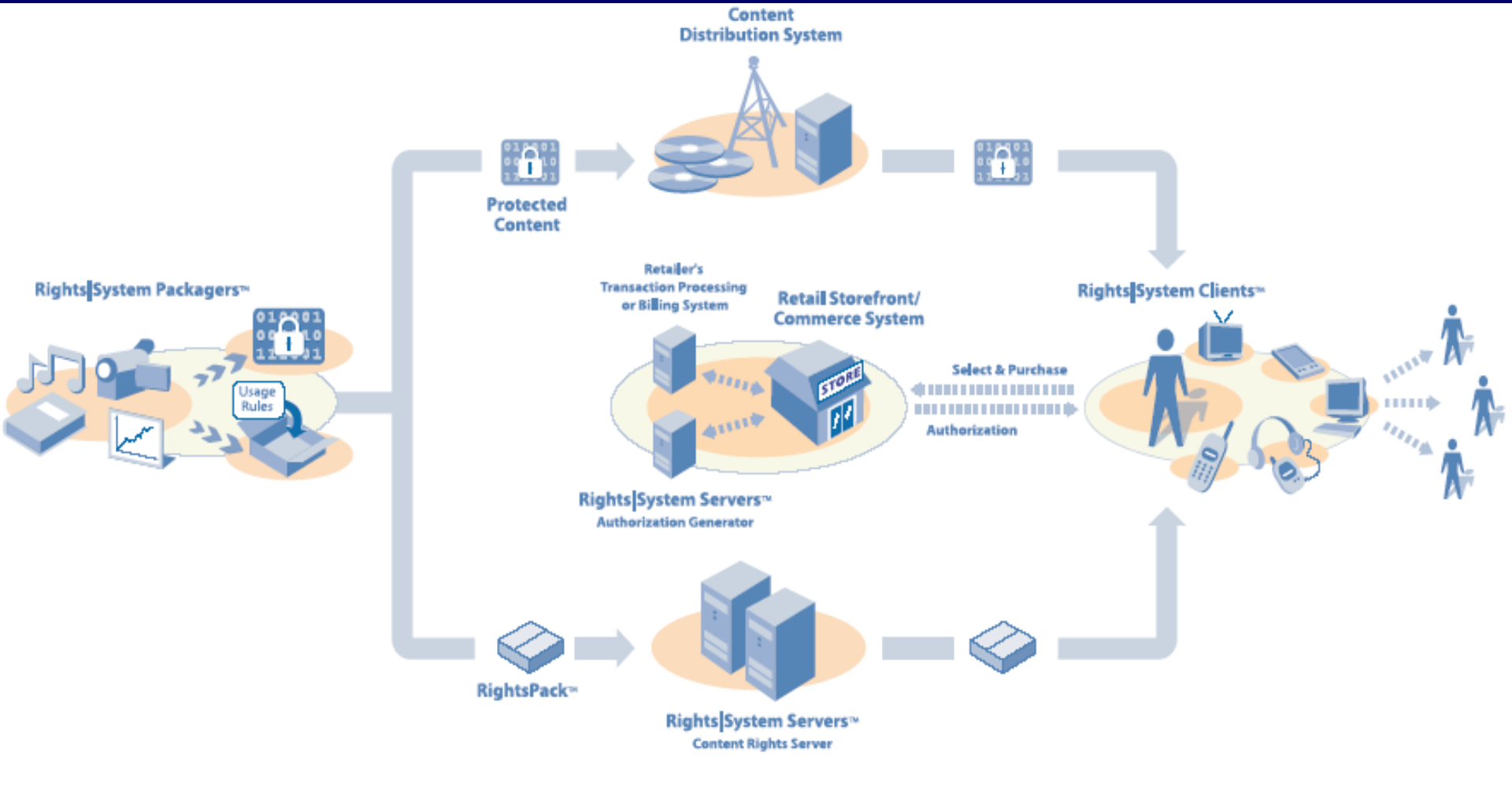
- Packager
  - Verpacken und Verschlüsseln digitaler Inhalte
  - erzeugt verschlüsselte Datei und sog. RightsPack (= Lizenz)
  - unterstützt gängige Dateiformate wie z. B. MP3, AAC, MPEG4 oder PDF
  - als Einzelanwendung lauffähig
  - konfigurierbar über XML-Eingabedatei
  - erweiterbar über Plugin-Mechanismus
- Server
  - Content Rights Server
  - Authorization Generator

Intertrust Rights|System

- **Clients**
  - **Clientsoftware für verschiedene Plattformen und Geräte**
    - ***Rights*|*Desktop* für PCs**
    - ***Rights*|*PD* für portable Endgeräte**
    - ***Rights*|*Phone* für Mobilfunkgeräte**
    - ***Rights*|*TV* für TV-Boxen**
- **Software Development Kit (SDK) erlaubt Softwareentwicklern,**
  - **DRM-Mechanismen von Intertrust in ihre Anwendungen einzubinden (z. B. *Rights*|*Audio SDK*)**
  - **oder an festdefinierten Stellen zu erweitern (z. B. *Packager SDK*)**

Intertrust Rights|System

- Funktionsweise des Rights|System



Weitere DRM-Lösungen

- Electronic Media Management Services (EMMS) von IBM
- Real One von Real Networks
- Adobe Content-Server
  - Für eBooks und PDF-Dokumente
  - Typische Nutzungsbeschränkungen:
    - Anzahl der Seiten, die betrachtet werden dürfen
    - ob das Dokument gedruckt werden darf
    - ob Teile des Dokumentes in die Zwischen-ablage des BS kopiert werden dürfen
    - wie lange das Dokument betrachtet werden darf

Schwächen von DRM-Schutzmechanismen

- Verwendung von „Hackerprogrammen“
  - Advanced Password Recovery
    - ermöglicht es, die in einer PDF-Datei hinterlegten DRM-Nutzungsbeschränkungen zu deaktivieren oder passwortgeschützte Dokumente zu öffnen
    - verwendet Lexika- und Bruteforce-Angriffe
    - bis Acrobat 4 einsetzbar
  - Unfuck.exe
    - konvertiert mit DRM1 kodierte Musikstücke in uneingeschränkte WMA-Dateien
    - bei der aktuellen DRM-Version ohne Wirkung

Schwächen von DRM-Schutzmechanismen

- Zeitliche Problematik
  - Schlüssellängen
  - Dateiformate
- Kein Schutz gegen analoge Kopien, z. B. Abgreifen der Audiodaten am analogen Ausgang der Soundkarte

  → Qualitätsverlust
- Abgreifen der Audiodaten am digitalen Ausgang der Soundkarte

  → kein Qualitätsverlust

Schwächen von DRM-Schutzmechanismen

- Audiorekorder
  - nutzen aus, dass die Audiodaten auf dem Weg zur Soundkarte entschlüsselt werden müssen
  - richten „virtuelle Soundkarte“ ein
  - fangen die entschlüsselten Daten ab
  - und schreiben sie auf Wunsch ohne Beschränkungen auf die Festplatte
  - Beispiele
    - Virtual Audio Cable und Total Recorder für Windows
    - vsound für Linux

Fazit

- DRM-Systeme haben für Anbieter und Rechteinhaber digitaler Güter einige Vorteile
  - ermöglichen Zugangs- und Nutzungskontrolle
  - gewährleisten die Authentizität und Integrität
  - ermöglichen ein automatisiertes Rechte-management
  - ermöglichen es, die kostengünstige technische Infrastruktur des Internet für den Vertrieb zu nutzen, zugleich aber die illegale Verbreitung durch Raubkopien einzuschränken

Fazit

- Zahlreiche Nachteile
  - in der Vergangenheit viele Schwächen
  - beim Kauf müssen persönliche Daten angegeben werden → hohes Risiko von Verletzungen des Datenschutzes und der Privatsphäre
  - Konzentration vorwiegend auf technische Sachverhalte → rechtliche, wirtschaftliche und soziale Gesichtspunkte oft nicht berücksichtigt
  - zu wenige Standards → einführungshemmend
  - wichtigste Komponente bleibt meist unberücksichtigt: **der Kunde**

Vielen Dank für Ihre Aufmerksamkeit!

Fragen ?