Digital Rights Management Systeme

Hannes Federrath
Universität Regensburg
Lehrstuhl Management der Informationssicherheit
http://www-sec.uni-regensburg.de/

Gliederung

- Einführung
- Offline-Distribution
  - Fall 1.1: Ungeschützter Inhalt auf Datenträger
  - Fall 1.2: Inhalt auf Datenträger mit Markierungen versehen
  - Fall 1.3: Spezielles nicht-konformes Speicherformat
  - Fall 2: Verschlüsselter Inhalt auf Datenträger
- Online-Distribution über das Internet
  - Schutzziele
  - Zugangskontrolle
  - Rechtemanagement und Kopierschutz
    - Fall 1: Unverschlüsselter und unmarkierter Inhalt
    - Fall 2: Markierter Inhalt
    - Fall 3: Verschlüsselter und markierter Inhalt
    - Fall 4: Verschlüsselter Inhalt
- Fazit

Fall 1.1: Ungeschützter Inhalt auf Datenträger

- Inhalt beliebig kopierbar:
  - Einlesen, speichern, vervielfältigen

Fall 1.2: Inhalt auf Datenträger mit Markierungen versehen

- Idee:
  - CD-Hersteller und Softwarehersteller einigen sich darauf, dass nur Spieler ausgeliefert werden, die eine Kopie als solche kennzeichnen.
  - Einlesen einer Kopie ist nicht erlaubt — nur das Abspielen.
- Hoffnung:
  - Kopie von Kopie kann nicht mehr angefertigt werden
  - Durchbrechen der Kopierkette
- Aber: Wo ist der Unterschied zwischen "Einlesen" und "Abspielen"?

Fall 1.2: Inhalt auf Datenträger mit Markierungen versehen

- Idee:
  - Man könnte eine gekennzeichnete Kopie zwar auslesen lassen, aber nicht wieder schreiben lassen.
- Realisierung z.B. durch
  a) Brennerhersteller oder
  b) SW-Hersteller (Brennersoftware)
- Problem:
  - Nicht alle Brennerhersteller werden sich an Regeln halten.
- Frage:
  - Wer stellt die Regel auf, wie werden Verstöße geahndet? Wie kommt man zu internationalen Regeln?
- Wenn Clonen des Datenträgers möglich ist, wird einfach das Kopierschutzkennzeichen mitkopiert.

Serial Copy Management System

digital audio player

digital audio

digital recorder

MD, CD-R (Audio), DAT

Free: copy bit is zero

0100101011101011101010011100110010

Protected Original: copy bit set

0100111011111011111010110111011100 11

Copy: content with copy bit alternating

0100111011101011110101001110111001 0

Serial Copy Management System

digital audio player

digital audio

digital recorder

MD, CD-R (Audio), DAT

Original

0100111011111011111010101101110111001 1

Copy

0100111011110101111010101011101110010

Reset copy bit to make copies

Copy

010011101110

010011101111

Original

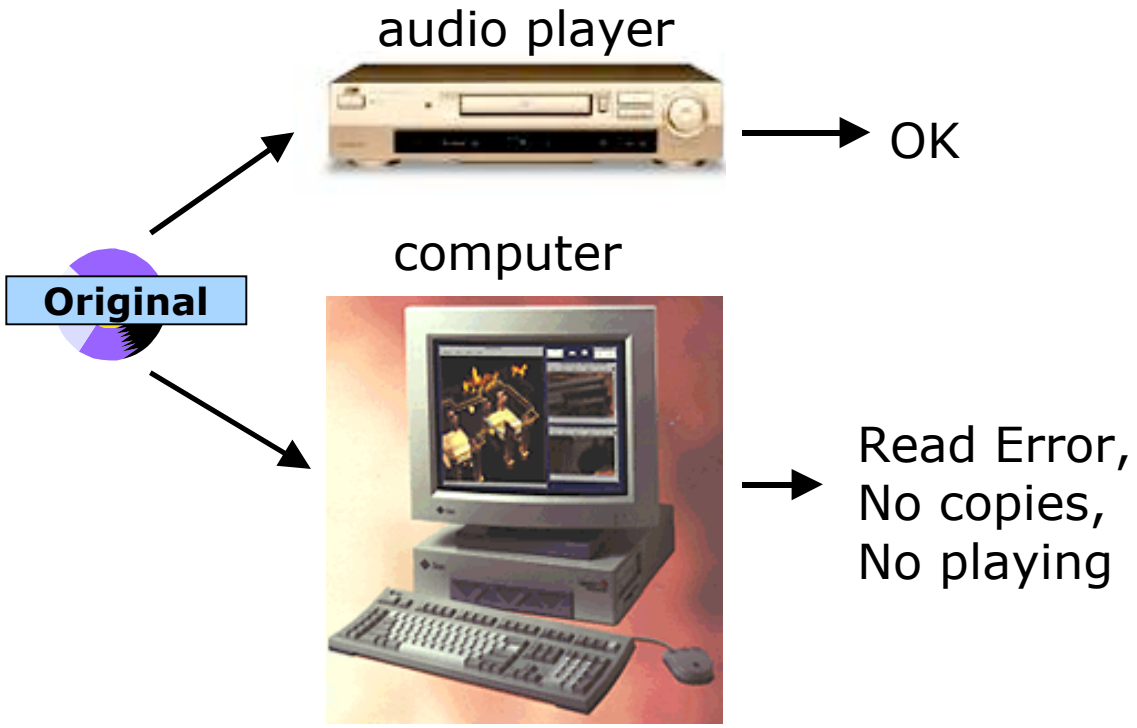
Fall 1.2: Inhalt auf Datenträger mit Markierungen versehen

- Spezielle Markierung:
  - Regionalcode bei DVD
    - Schutz wird durch Player (Hardware) realisiert
    - Soll Nutzung auf bestimmte Territorien beschränken
- Problem auch hier:
  - Region-Code-freie Abspielgeräte
- Selbst dann, wenn sich alle Brennerhersteller daran halten würden:
  - SW-Hersteller sind nicht kontrollierbar
  - Jeder kann Programm schreiben, das die Kennzeichnung entfernt

Fall 1.3: Spezielles nicht-konformes Speicherformat

- Nutzt unterschiedliche Spezifikation von CD-ROM und CDDA aus.
  - Kompatibilität ist eigentlich durch Standard garantiert.
- Schutzidee 1:
  - Musik-CD wird vom CD-Hersteller in einem nicht Standard-konformen Format geschrieben
  - Einbringen von Fehlerstellen insb. in der Verzeichnisstruktur, die nur vom CD-ROM-Laufwerk gelesen wird
- Problem:
  - Modernere Audio-Spieler nutzen die wegen der Massenverbreitung billigeren CD-Laufwerke in ihren Playern.
- Folge:
  - Nicht Standard-konforme CDs spielen nicht mehr.
- Kopieren ist durch Clonen meist trotzdem möglich
  - Fehler werden einfach ebenfalls dupliziert

Fall 1.3: Spezielles nicht-konformes Speicherformat



Fall 1.3: Spezielles nicht-konformes Speicherformat

Fall 1.3: Spezielles nicht-konformes Speicherformat

- Schutzidee 2:
  - Original-CD enthält Daten, die zwar gelesen, aber bisher nicht geschrieben werden können (z.B. Spezielle Spuren)

- Problem:
  - Irgendein Brennerhersteller wird früher oder später einen Brenner anbieten, der auch diese Daten schreiben kann.

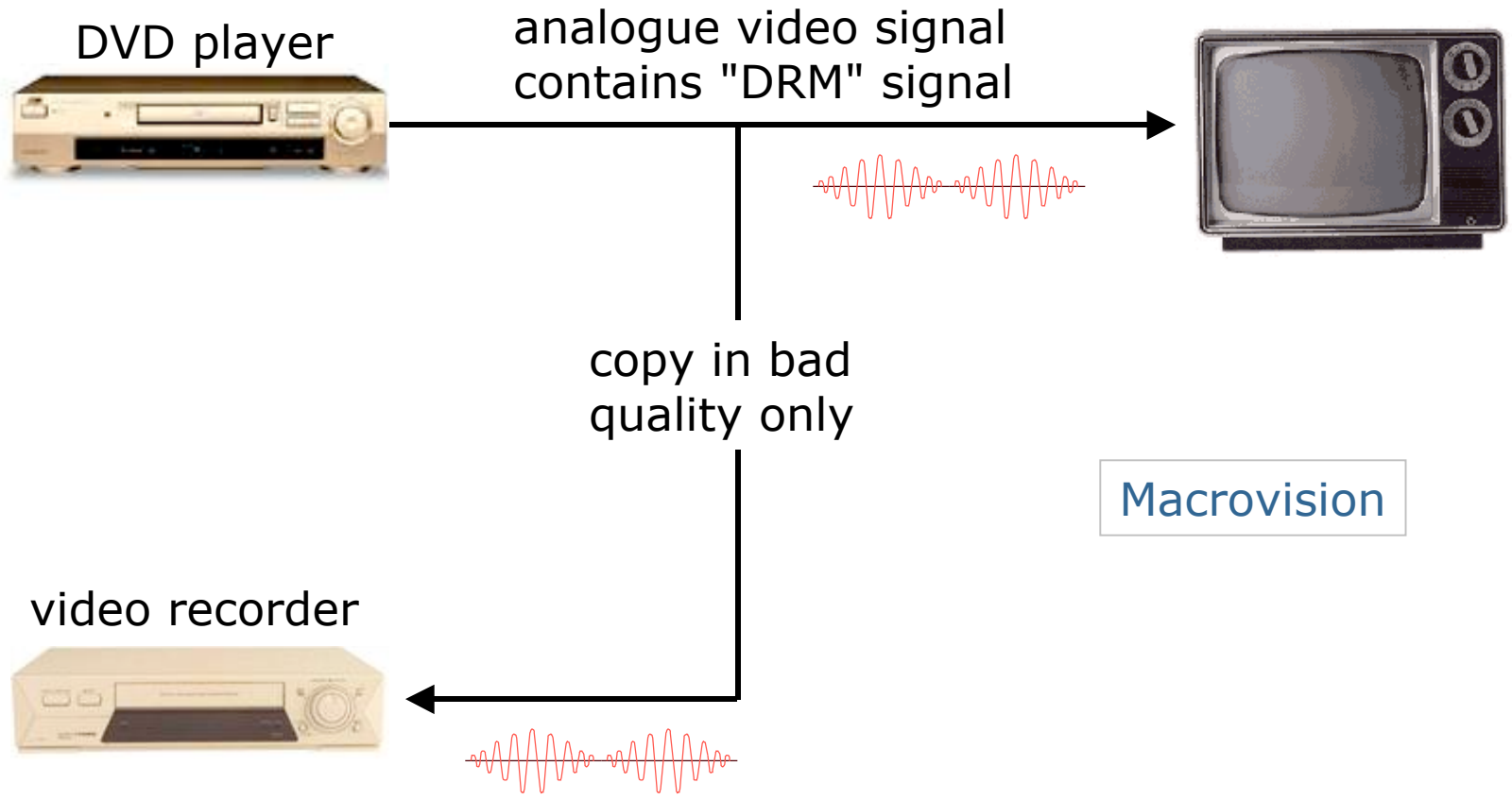
Fall 2: Verschlüsselter Inhalt auf Datenträger

- Vorbemerkung:
  - Das Folgende macht nur Sinn, wenn Clonen des Datenträgers nicht möglich ist.
- Schutzmöglichkeiten am Beispiel DVD
  1. Schlüssel ist im Abspielgerät
  2. Personalcomputer entschlüsselt

- Verfahren in der Analogwelt
  - Macrovison Kopierschutz
- Idee
  - Inhalt lässt sich hochqualitativ auf Fernseher ausgeben, aber nicht analog aufzeichnen
  - Vorverstärker eines Videorekorders erkennt Kopierschutzsignal
- Problem
  - Kopierschutzsignal kann leicht aus Analogsignal "herausgefiltert" werden

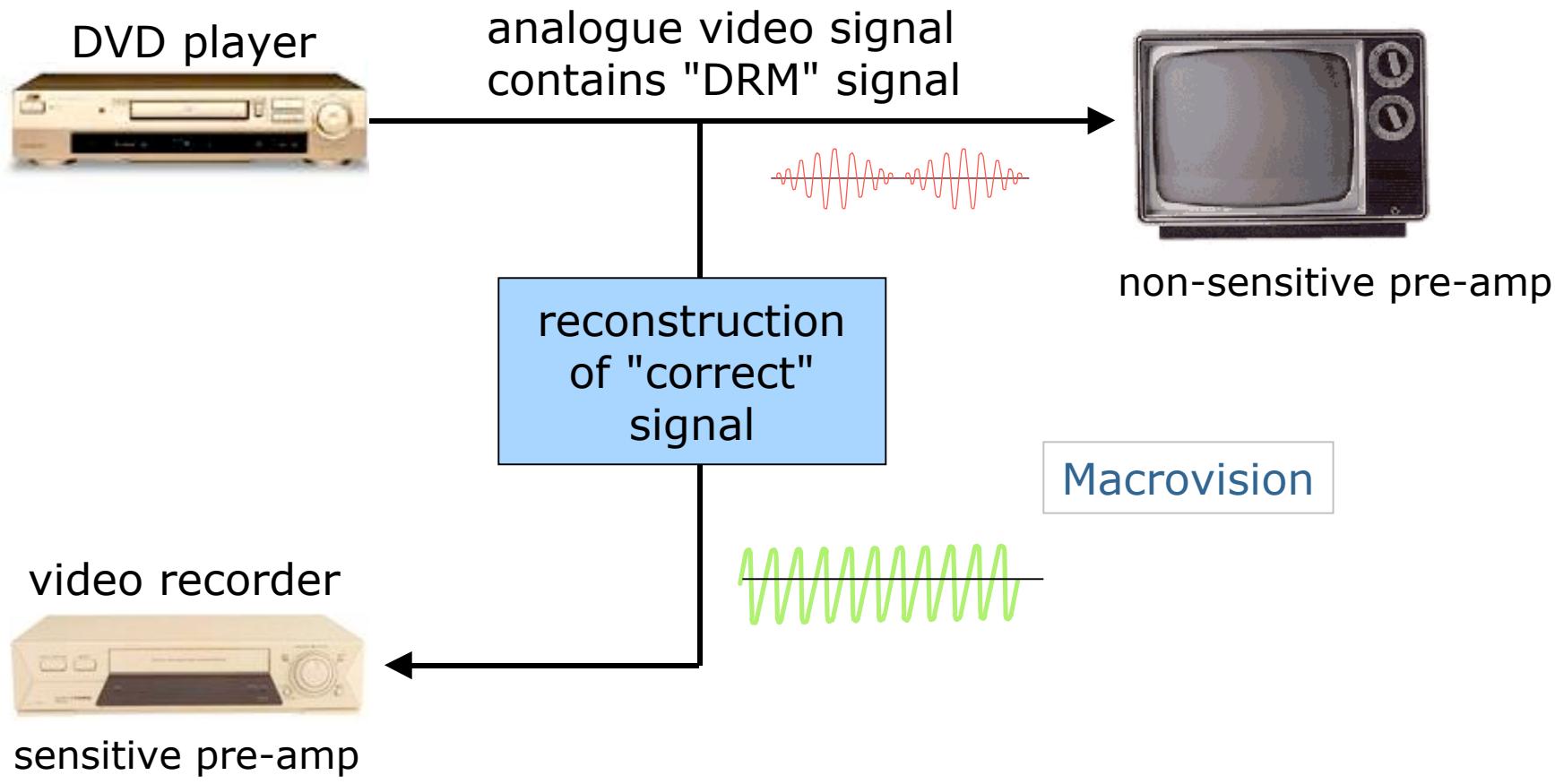
Macrovison Kopierschutz

- Schlüssel ist im Abspielgerät
  - Player gibt die Inhalte in niedriger Qualität aus



Macrovison Kopierschutz

- Schlüssel ist im Abspielgerät
  - Player gibt die Inhalte in niedriger Qualität aus



Fall 2: Verschlüsselter Inhalt auf Datenträger

- Personalcomputer:
  - muss gewährleisten,
    - dass unverschlüsselte digitale Daten nur an autorisierte Abspielprogramme weitergegeben werden und
    - nicht unverschlüsselt abgespeichert werden dürfen
  - praktisch mit heutigen PC-Architekturen nicht machbar

- Angriff auf digitale Daten:
  - Wer den Schlüssel aus einem Gerät (illegal) auslesen kann, kann jeden Inhalt entschlüsseln.
    - Angriffstool bei verschlüsselten DVDs: DeCSS
  - Brute-Force-Angriff auf Medienschlüssel

Fall 2: Verschlüsselter Inhalt auf Datenträger

- Ansätze für die Zukunft:
  - Player:
    - Völlig neue Spielergeneration als Voraussetzung für "neue" Datenträger
  - PC:
    - Spezielle Hardware, die im PC eingebaut ist, schützt vor Ausführung nicht autorisierter Programme.

(siehe später)

Zusammenfassung Offline-Distribution

- Stärke der existierenden Verfahren
  - erschweren das Kopieren,
  - können es aber nicht verhindern
- Es ist kein System in Sicht, das Kopieren wirklich verhindert.
- Folge:
  - technisch nicht befriedigend kontrollierbar, wer in welchem Umfang urheberrechtlich geschützte Inhalte kopiert

Gliederung

- Einführung
- Offline-Distribution
  - Fall 1.1: Ungeschützter Inhalt auf Datenträger
  - Fall 1.2: Inhalt auf Datenträger mit Markierungen versehen
  - Fall 1.3: Spezielles nicht-konformes Speicherformat
  - Fall 2: Verschlüsselter Inhalt auf Datenträger
- Online-Distribution über das Internet
  - Schutzziele
  - Zugangskontrolle
  - Rechtemanagement und Kopierschutz
    - Fall 1: Unverschlüsselter und unmarkierter Inhalt
    - Fall 2: Markierter Inhalt
    - Fall 3: Verschlüsselter und markierter Inhalt
    - Fall 4: Verschlüsselter Inhalt
- Fazit

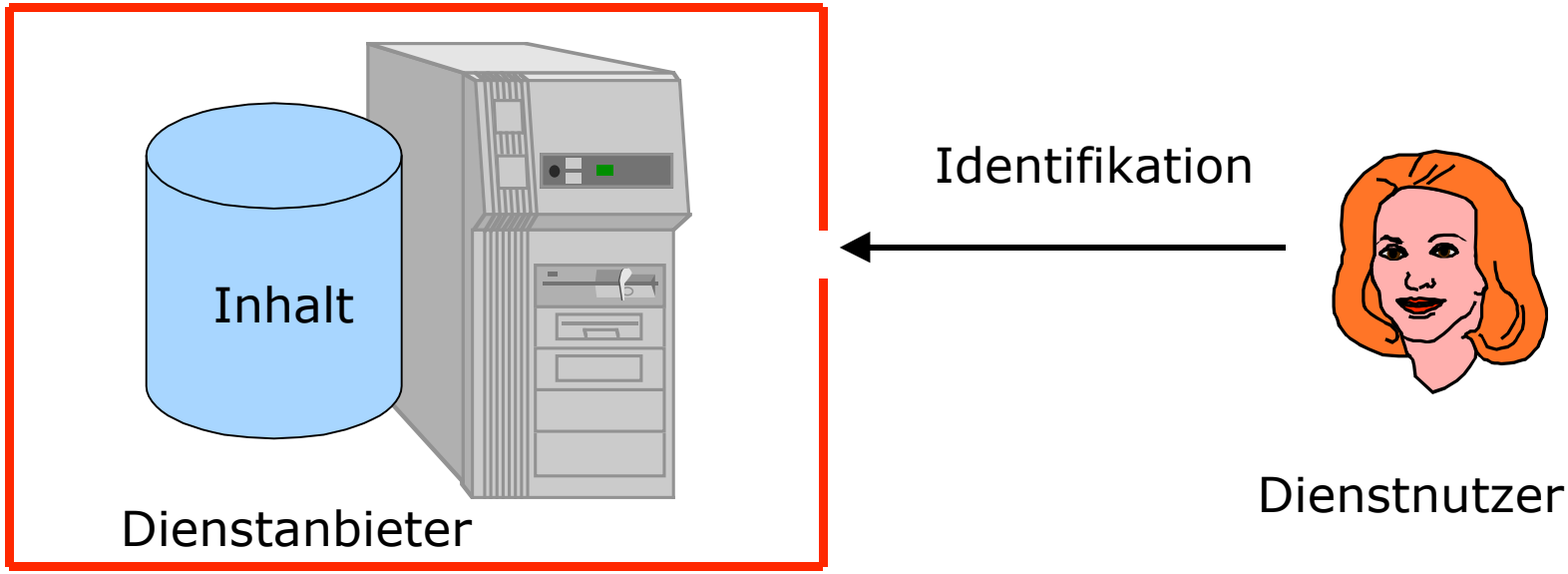
Schutzziele bei der Online-Distribution

- Schutzziel
  - Inhalte sollen nur von Berechtigten (die für den Inhalt bezahlt haben), genutzt werden können
- Mechanismus
  - Zugangskontrolle

- Schutzziel
  - Inhalte sollen nur in der vereinbarten Weise genutzt werden können
- Mechanismus
  - DRM-Systeme

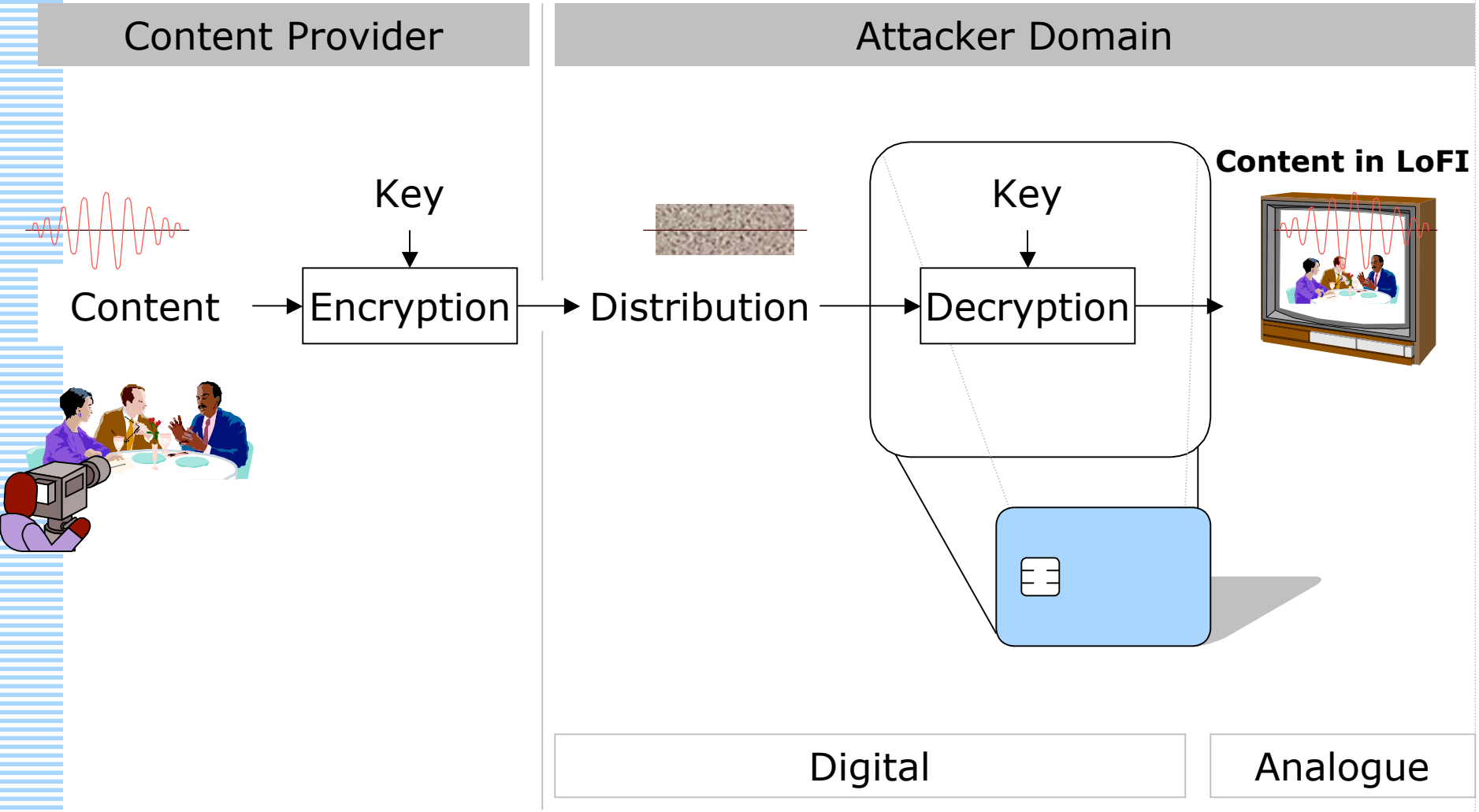
Zugangskontrolle

- IT-System erfragt die Identitäten seiner Kommunikationspartner
- Zweck
  - Nur mit berechtigten Partnern weiter kommunizieren
  - Verhindert unbefugte Inanspruchnahme von Betriebsmitteln



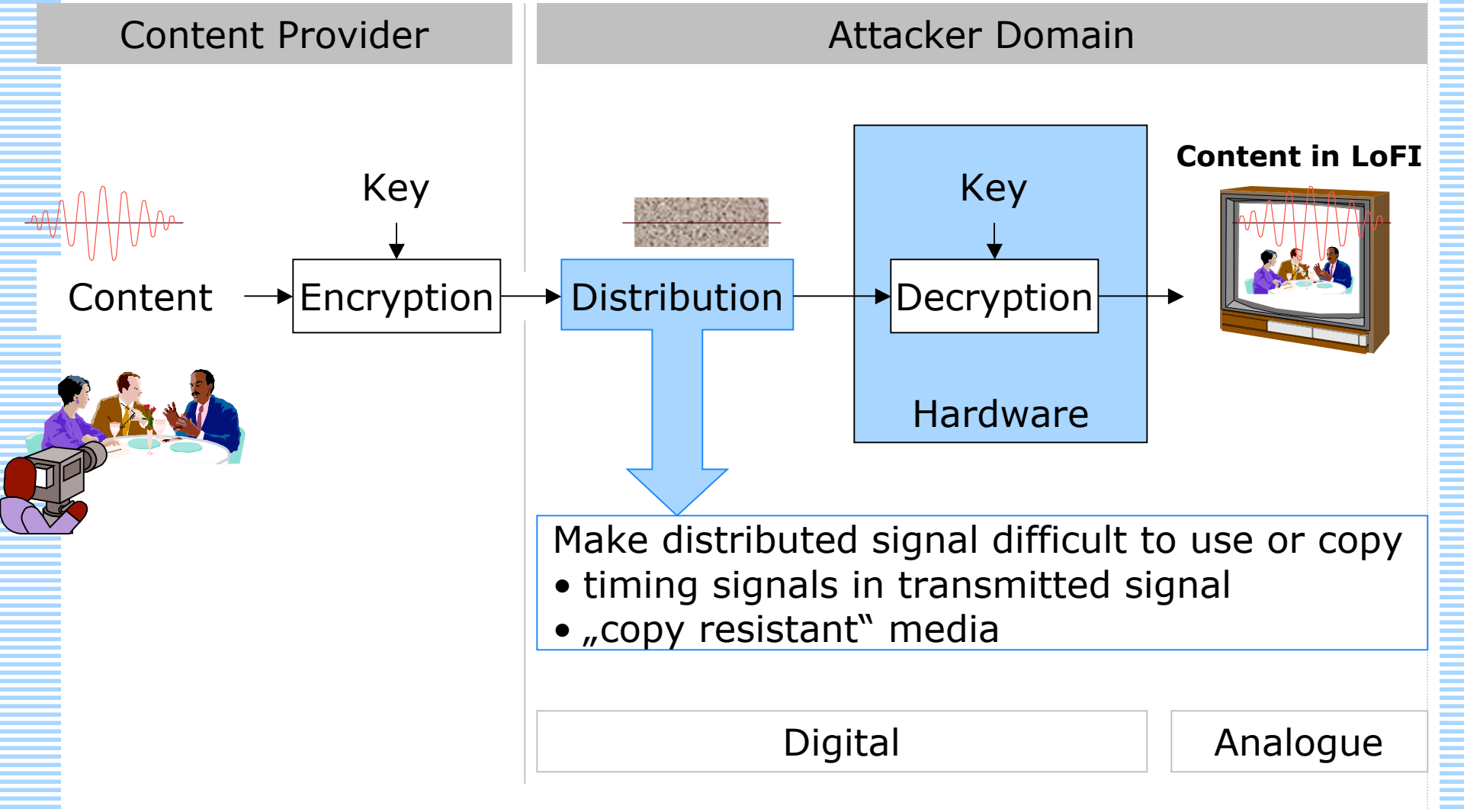
Design Options for Copy Protection

- Protect pay-services from unauthorized access

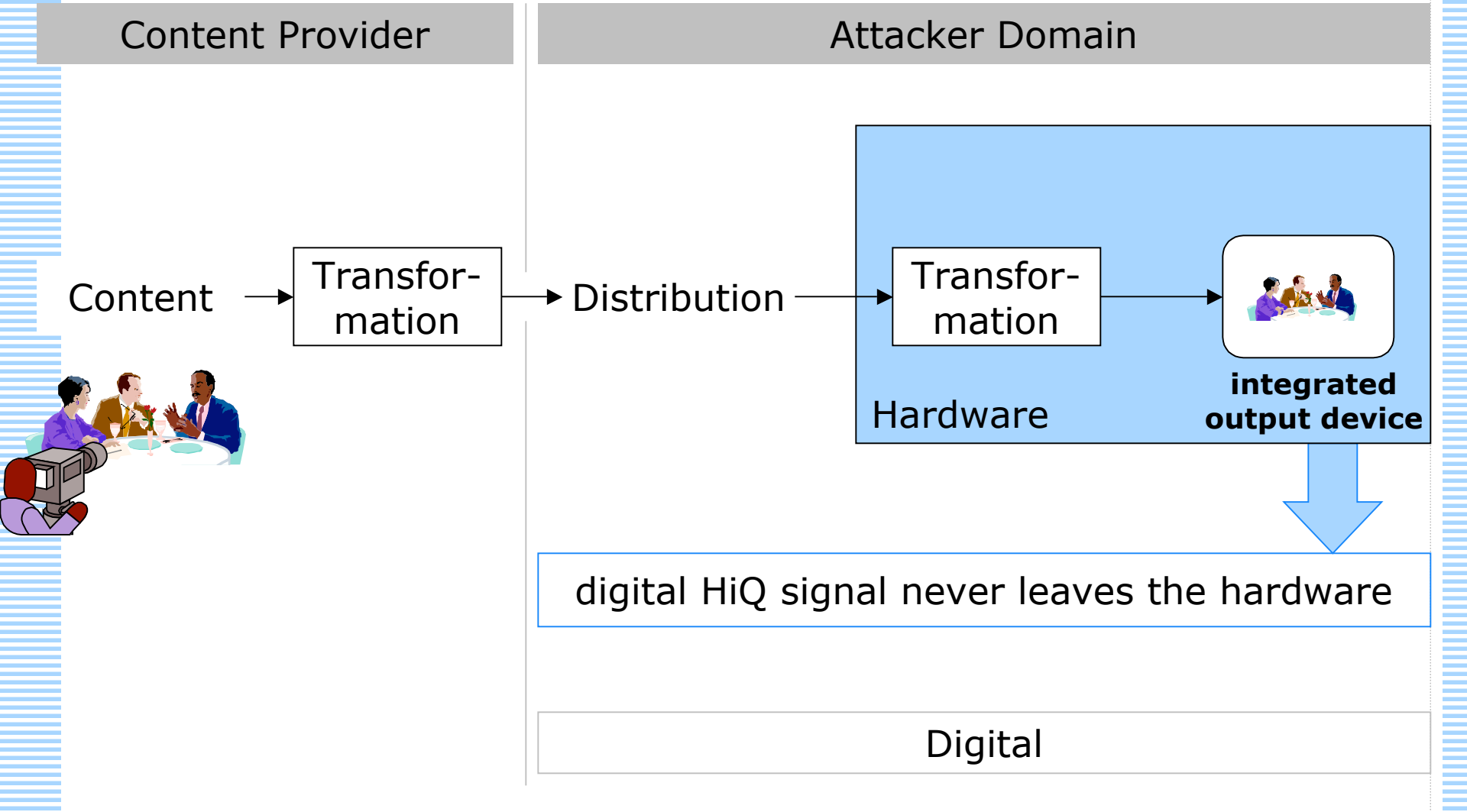


Design Options for Copy Protection

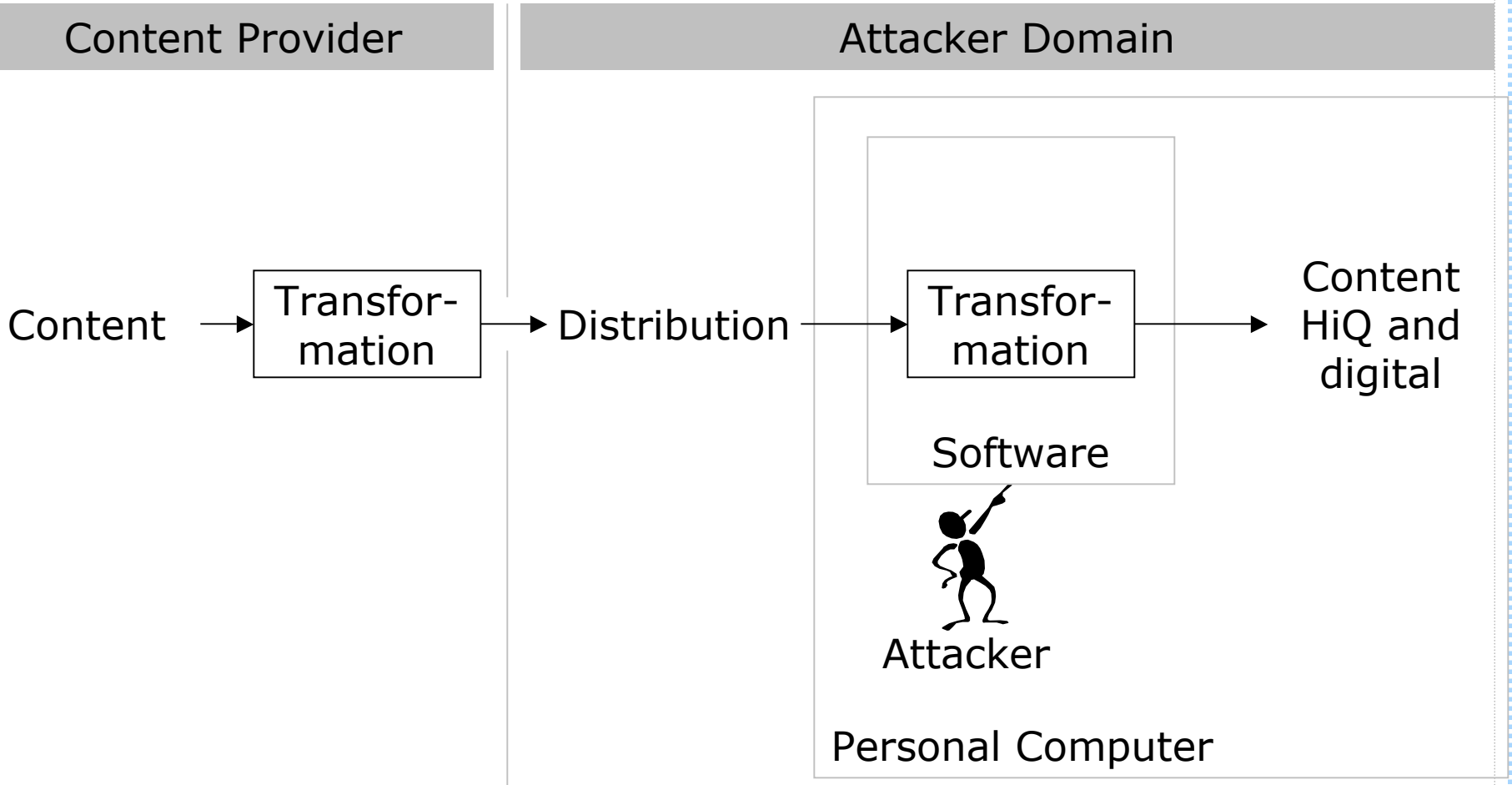
- Protect pay-services from unauthorized access



Design Options for Copy Protection



Never! Too dangerous!



Gliederung

- Einführung
- Offline-Distribution
  - Fall 1.1: Ungeschützter Inhalt auf Datenträger
  - Fall 1.2: Inhalt auf Datenträger mit Markierungen versehen
  - Fall 1.3: Spezielles nicht-konformes Speicherformat
  - Fall 2: Verschlüsselter Inhalt auf Datenträger
- Online-Distribution über das Internet
  - Schutzziele
  - Zugangskontrolle
  - Rechtemanagement und Kopierschutz
    - Fall 1: Unverschlüsselter und unmarkierter Inhalt
    - Fall 2: Markierter Inhalt
    - Fall 3: Verschlüsselter und markierter Inhalt
    - Fall 4: Verschlüsselter Inhalt
- Fazit

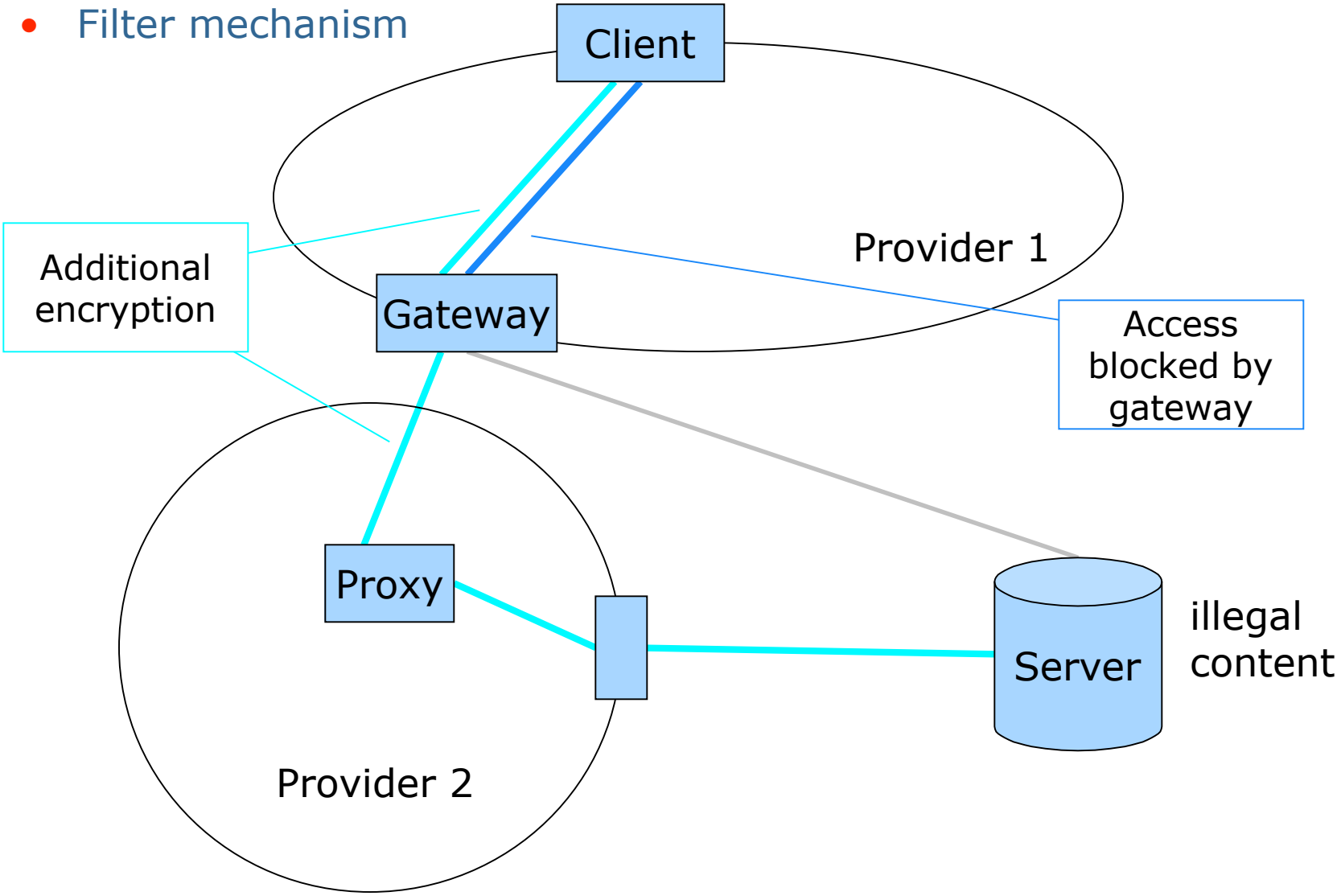
Fall 1: Unverschlüsselter und unmarkierter Inhalt

- Kein Schutz:
  - technisch gesehen beliebig kopier- und nutzbar

- Naiver Mechanismus
  - Filter zur Zugriffsbeschränkung
    - auf illegale Inhalte
    - zur territorialen Zugriffsbeschränkung

Bypassing Rights Protection System (RPS)

- Filter mechanism

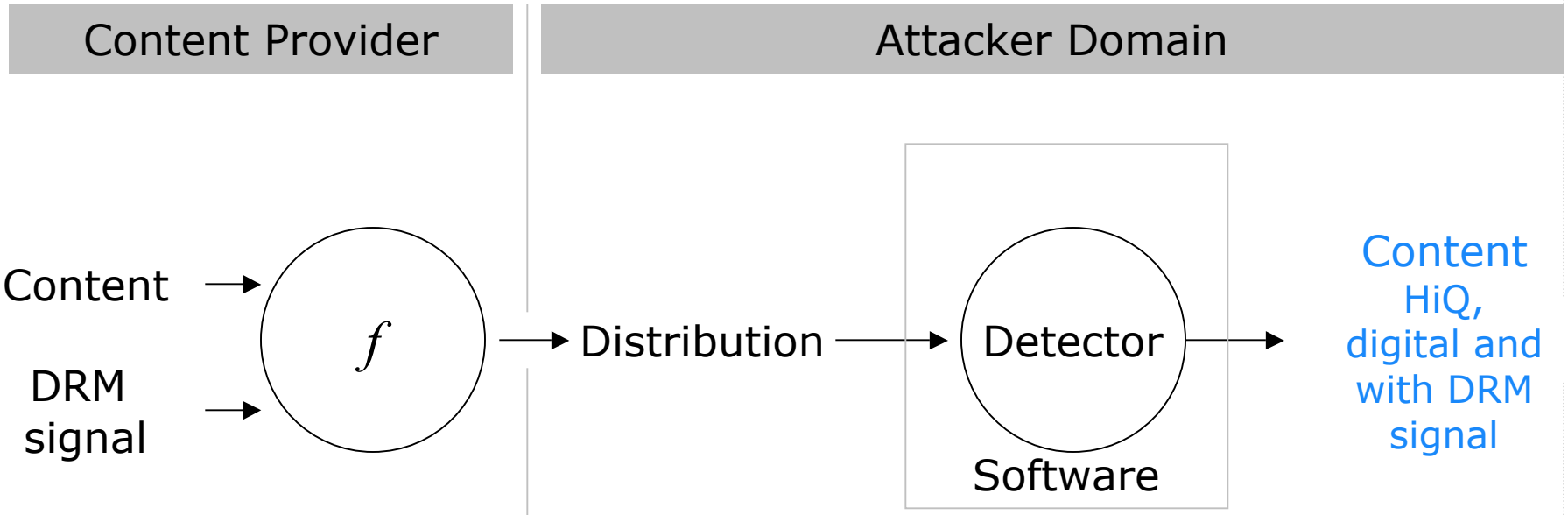


Fall 2: Markierter Inhalt

1. Kennzeichnung des Urhebers:
   - Verhindert, dass Inhalte unbemerkt als die eigenen ausgegeben werden können.
   - Bzgl. Vergütungsmodellen von untergeordneter Bedeutung.
2. Kennzeichnung des Käufers:
   - Verhindert, dass Inhalte unbemerkt weitergegeben werden können.

- Schutzidee:
  - Einbringen eines schwer entfernbaren "Watermarks" in den Inhalt
  - Für 2.: Setzt individuelle Kopien des Inhalts voraus

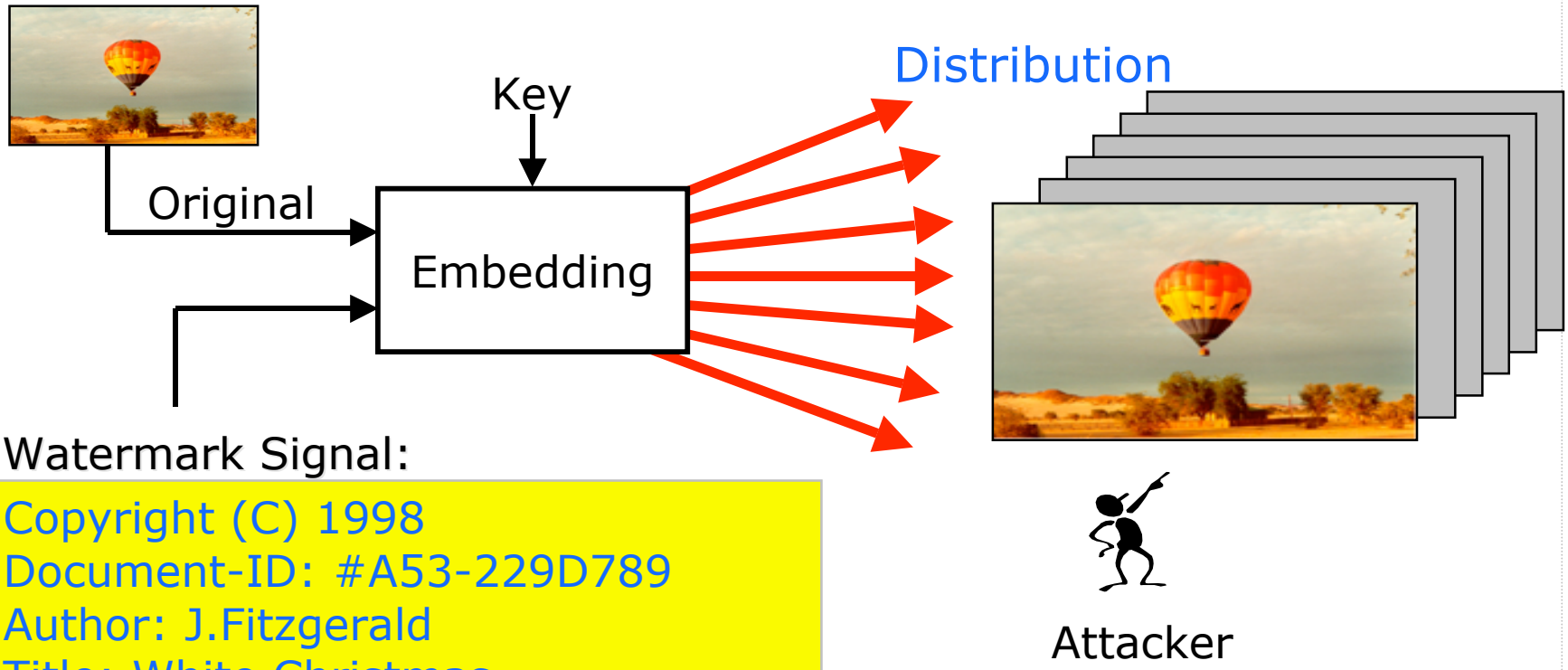
Watermarking



- Watermarking:
  - Goal: Protection of authorship
  - Not: Protection against illegal copying
  - Possible: Detection of copies

Digital

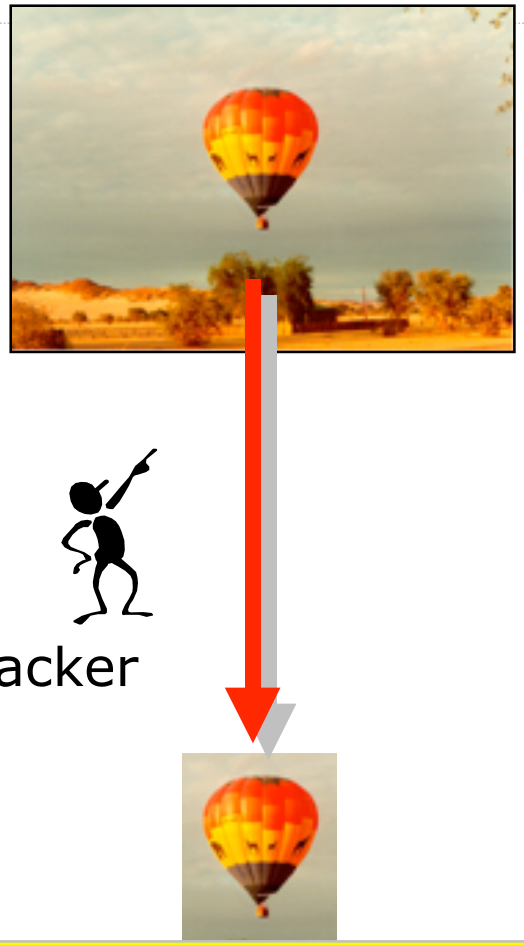
Watermarking



> Watermarking

- Digital-Analogue-Conversion
- Analogue-Digital-Conversion
- Re-Sampling
- Re-Quantization
- Compression
- Dithering
- Rotation
- Translation
- Cropping
- Scaling

- Collusion Attacks



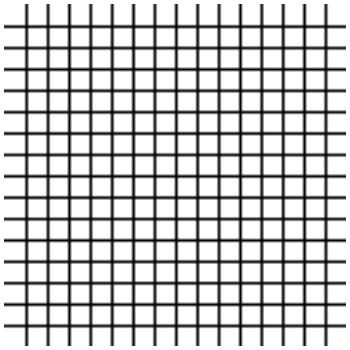
> Security of watermarking systems

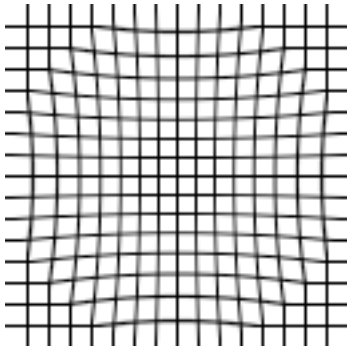
- Theory
  - robustness
  - non-interference
  - detectability

- Praxis: (attacks by M. Kuhn, F. Petitcolas, 1997)
  - StirMark
    - Software
    - removes watermarks
    - watermark is no longer detectable
    - http://www.cl.cam.ac.uk/~fapp2/watermarking/stirmark/
  - Mosaic Attack
    - divides web images into a mosaic of tabular cells
    - browser reconstructs the view of the image

Stirmark Attack

- non-linear transformation of a picture
- synchronization gets lost
- no anchor for detector to find the position of embedded signal





Mosaic Attack

- divides web images into a mosaic of tabular cells
- uses html statements
- browser reconstructs the view of the image
- protects from very simple web robots that look for illegally distributed material

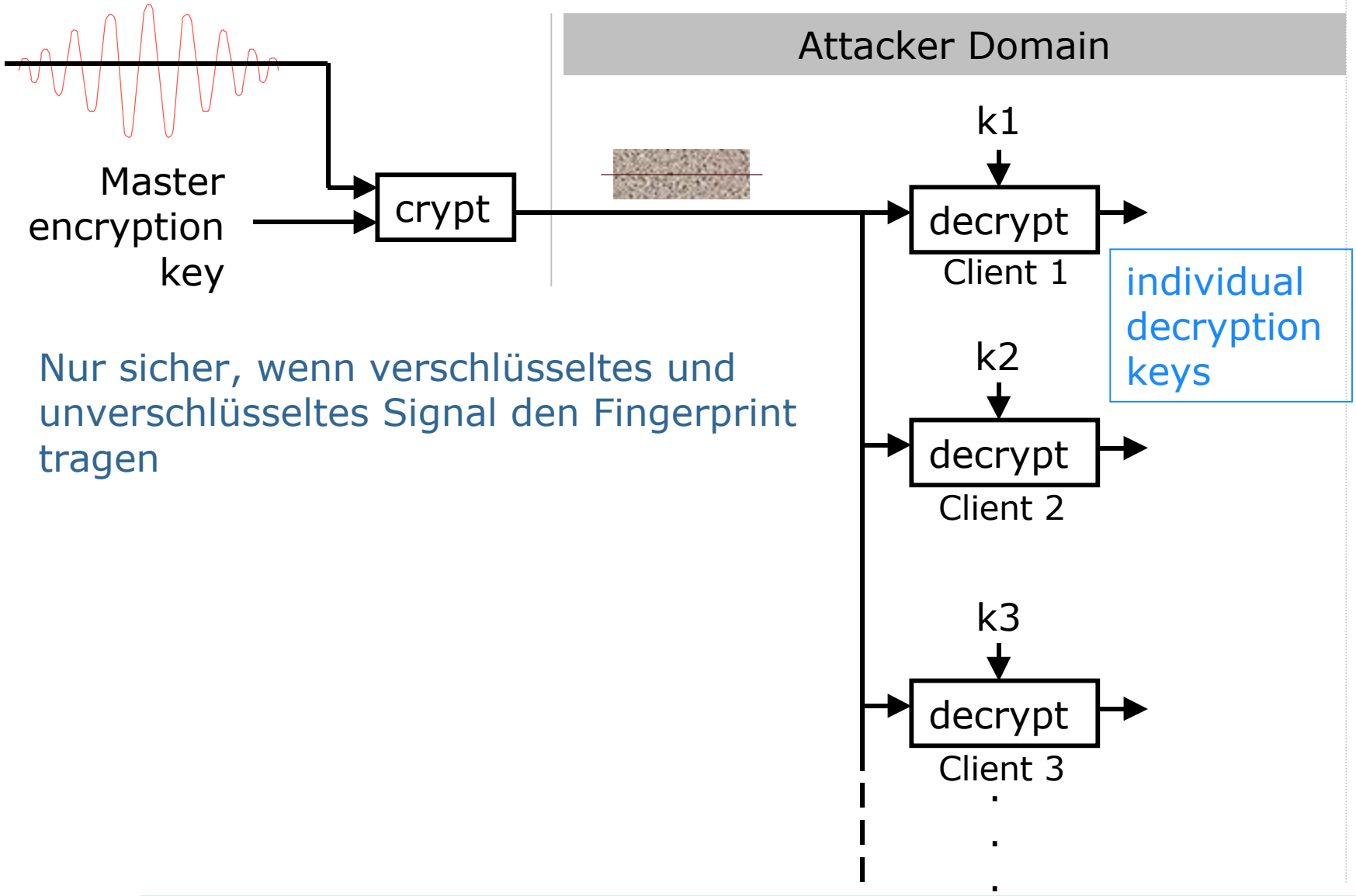
Fall 3: Verschlüsselter und markierter Inhalt

- Ebenfalls Kennzeichnung des Käufers
  - Fingerprinting

- Schutzidee:
  - Schlüssel wird gekennzeichnet
  - Ermöglicht Verfolgung der Schlüsselweitergabe

  - Individuelle Schlüssel, aber keine individuellen Inhalte
  - Broadcast Encryption, sehr aufwendig

Broadcast encryption



- Nur sicher, wenn verschlüsseltes und unverschlüsseltes Signal den Fingerprint tragen

Fall 4: Verschlüsselter Inhalt

- Vorbemerkung:
  - Das Folgende gilt auch für Fall 3.
- Schutzziel:
  - Es muss sichergestellt werden, dass der Inhalt nur in der vorgesehenen Weise genutzt wird.
- Nutzungsarten: Beispiele:
  - X-mal nutzen (anschauen, anhören, ...) mit X>=1
  - Y-mal kopieren (z.B. auf CD) mit Y>=0
  - nur in Territorium Z nutzbar
  - nur bis zum Zeitpunkt T nutzbar
- Realisierung
  - DRM-Systeme

DRM-Systeme heute

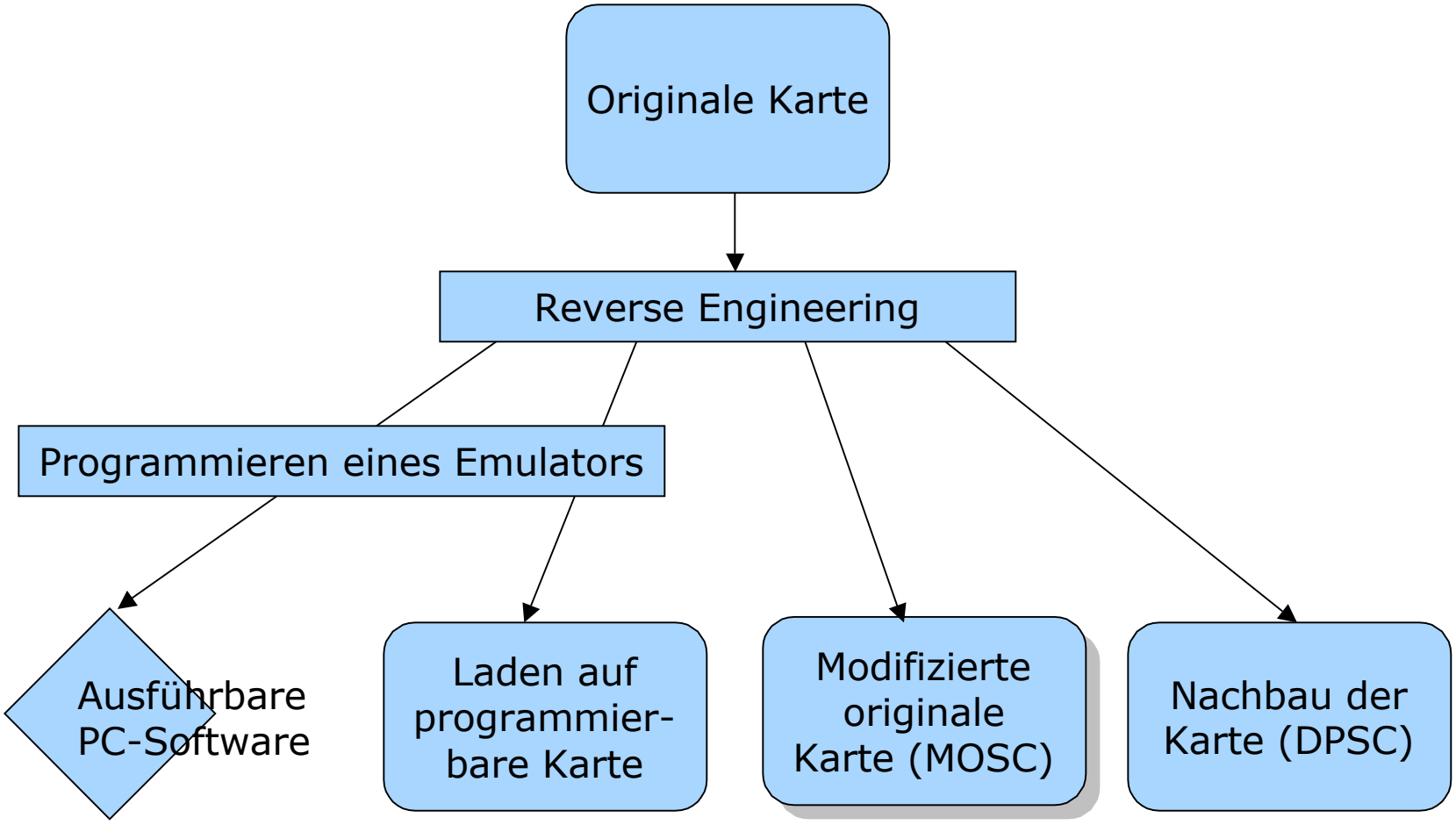
- Realisierungsansatz:
  - Inhalt wird um Meta-Daten ergänzt
  - Meta-Daten tragen Informationen über die erlaubten Nutzungsarten
  - "Offizielle" Abspielsoftware liest Meta-Daten und gibt Inhalte für erlaubte Nutzungsarten frei

- Problem:
  - Geräte, auf denen Inhalte heute typischerweise genutzt werden:
    - frei programmierbarer Universal-PC
    - umprogrammierbare Set-Top-Box

Frei programmierbarer Universal-PC

- Angriff:
  - Anstelle der "offiziellen" Nutzungssoftware wird fremde Software genutzt, die die Nutzungsmöglichkeiten nicht einschränkt.
  - Das ist nicht verhinderbar!
- Vorgehen aus Angreifersicht:
  - Reverse Engineering des offiziellen Programms.
- Beispiele:
  - RealPlayer-Modifikation mit Abspeicherfunktion
  - DRM von Microsoft
  - E-Book-Software von Adobe
  - Abonnenten-TV

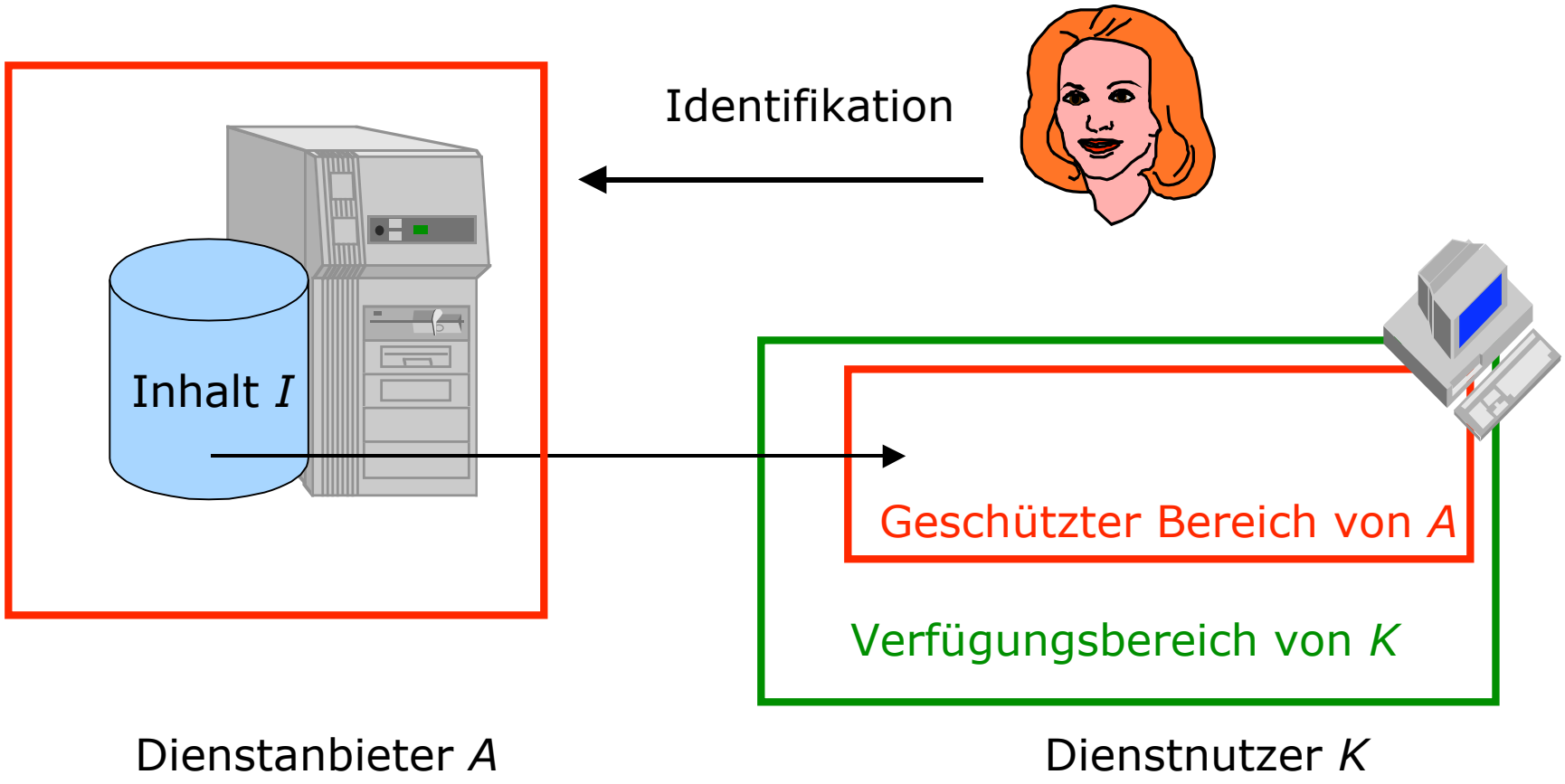
Angriffe im Bereich Pay-TV



z.B.
Multidec+Soft-CI-DLL

Das DRM-Problem

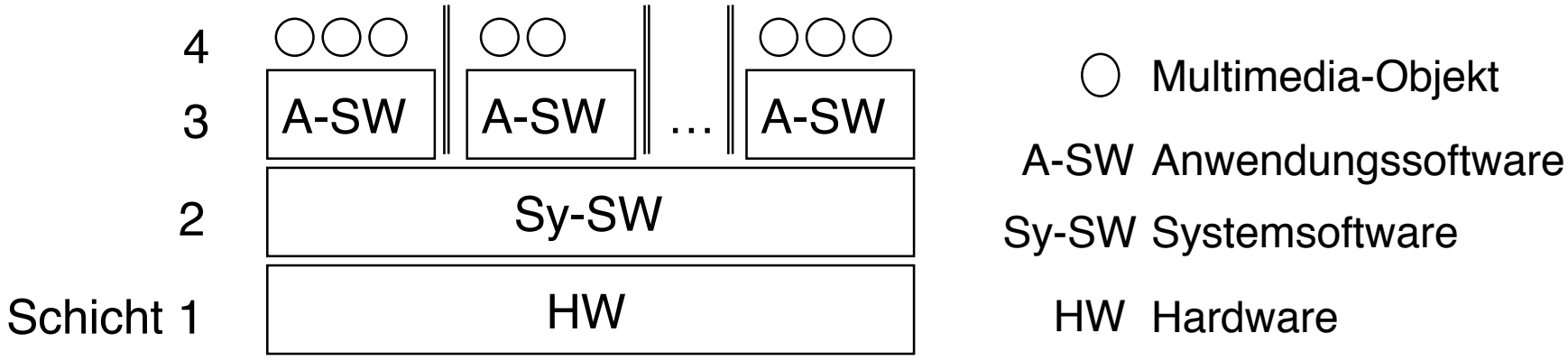
- Einem Kunden *K* einen Inhalt *I* in einer bestimmten Weise zugänglich machen, ihm aber daran hindern, *alles* damit tun zu können.



Frei programmierbarer Universal-PC

- Ausführungs-Schichtenstruktur
  - Objekte können vor den darunter liegenden Schichten nicht effizient geschützt werden.

- Folge:
  - Auf frei programmieren PCs werden Multimedia-Objekte nie wirklich schützbar sein.



[Nicht] Frei programmierbarer Universal-PC

- Abwehr:
  - spezielle Hardware (Tamper Proof Module, TPM), die im PC eingebaut ist
  - schützt vor Ausführung nicht autorisierter Programme
- Folge:
  - Es können nur noch offizielle Programme mit einem geschützten Inhalt verwendet werden.
- Beachte:
  - Autorisierung muss bis auf Hardware-Treiber-Ebene erfolgen!

- Grundproblem:
  - Selbst Hardwaremodul bietet nicht ewig Sicherheit.
- Hoffnung:
  - Zeitraum, über den das Geheimnis geschützt bleibt, ist länger als Schutzbedarf des Inhalts

Nicht frei programmierbarer Universal-PC

- Zu beachten:
  1. Entweder: Inhalte werden in Hardwaremodul entschlüsselt
  2. Oder: Server darf unverschlüsselte Inhalte erst nach Autorisierung durch das Hardwaremodul ausgeben.

  - Bei 2. muss Content-Server die Authentizität des Hardwaremoduls überprüfen
  - Weder 1. noch 2. momentan in der Spezifikation des Hardwaremoduls der TCG (früher TCPA) vorgesehen.

- Datenschutzsicht
  - Funktionen zur Identitätsprüfung durch Content-Server sind wegen der Erstellungsmöglichkeit von Nutzungsprofilen nicht zu empfehlen.
  - siehe z.B. Diskussionen bzgl. Prozessor-IDs auf Intel-Chips

Gliederung

- Einführung
- Offline-Distribution
  - Fall 1.1: Ungeschützter Inhalt auf Datenträger
  - Fall 1.2: Inhalt auf Datenträger mit Markierungen versehen
  - Fall 1.3: Spezielles nicht-konformes Speicherformat
  - Fall 2: Verschlüsselter Inhalt auf Datenträger
- Online-Distribution über das Internet
  - Zugangskontrolle
  - Rechtemanagement und Kopierschutz
    - Fall 1: Unverschlüsselter und unmarkierter Inhalt
    - Fall 2: Markierter Inhalt
    - Fall 3: Verschlüsselter und markierter Inhalt
    - Fall 4: Verschlüsselter Inhalt
- Fazit

Strength of existing systems

- Very limited protection
  - Most systems
    - protect against hobbyists
  - DRM systems realized in software
    - no or nearly no protection against serious attacks
  - DRM systems realized in hardware
    - weak protection against serious attacks

- In the best case:
  - Technical components of DRM systems consist of special adapted and well-known IT security functions
- Worst case:
  - Content contains proprietary DRM signals or functions without any special protection

Digital Rights Management Systeme

Hannes Federrath
Universität Regensburg
Lehrstuhl Management der Informationssicherheit
http://www-sec.uni-regensburg.de/