# Grenzen des technischen Urheberrechtsschutzes

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

IT-Sicherheitsmanagement
Prof. Dr.-Ing.
Hannes Federrath

## Management der Informationssicherheit

IT-Sicherheitsmanagement versucht, die mit Hilfe von Informationstechnik (IT) realisierten Produktions- und Geschäftsprozesse in Unternehmen und Organisationen systematisch gegen beabsichtigte Angriffe (Security) und unbeabsichtigte Ereignisse (Safety) zu schützen.

- Themen, die am Lehrstuhl bearbeitet werden:
  - Sicherheit in verteilten Systemen und Mehrseitige Sicherheit
  - Datenschutzfreundliche Techniken
  - Sicherheit im Internet
  - Digital Rights Management Systeme
  - Sicherheit im E-Commerce und in mobilen Systemen
- Weitere Informationen:
  - http://www-sec.uni-regensburg.de

## Gliederung

- 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
  - Fall 1: Unverschlüsselter und unmarkierter Inhalt
  - Fall 2: Markierter Inhalt
  - Fall 3: Verschlüsselter und markierter Inhalt
  - Fall 4: Verschlüsselter Inhalt
- Fazit

IT-Sicherheitsmanagement
Prof. Dr.-Ing. Hannes Federrath

## Fall 1.1: Ungeschützter Inhalt auf Datenträger

- Inhalt beliebig kopierbar:
  - Einlesen, speichern, vervielfältigen

## Fall 1.2: Inhalt auf Datenträger mit Markierungen versehen

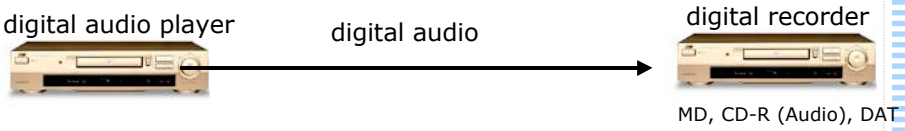
- Idee:
  - CD-Hersteller und Softwarehersteller einigen sich darauf, dass nur Spieler ausgeliefert werden, die eine Kopie als solche kennzeichnen.
  - Einlesen einer Kopie ist nicht erlaubt — nur das Abspielen.
- Hoffnung:
  - Kopie von Kopie kann nicht mehr angefertigt werden
  - Durchbrechen der Kopierkette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

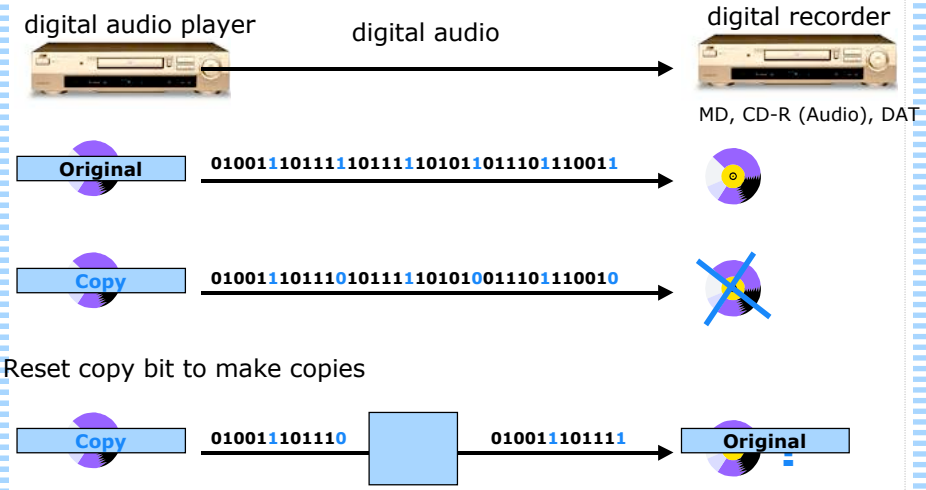



Free: copy bit is zero — 0100101011101011101010011100110010

Protected Original: copy bit set — 0100111011111011111010110111011100111

Copy: content with copy bit alternating — 0100111011101011110101001110111001 0

## Serial Copy Management System

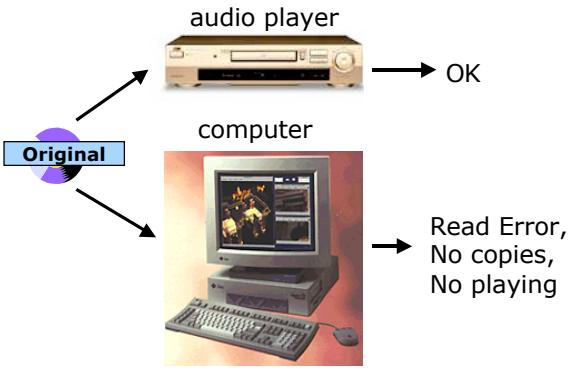





## Fall 1.3: Spezielles nicht-konformes Speicherformat

- 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




IT-Sicherheitsmanagement
Prof. Dr.-Ing. Hannes Federrath

## 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.

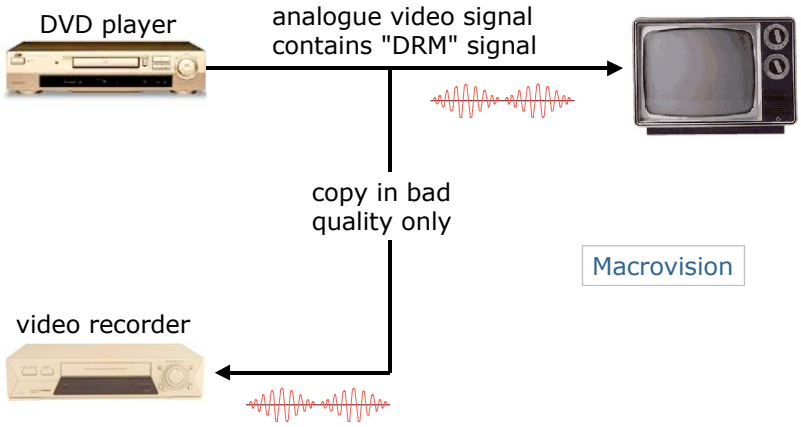


## Fall 2: Verschlüsselter Inhalt auf Datenträger

- 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

## Fall 2: Verschlüsselter Inhalt auf Datenträger

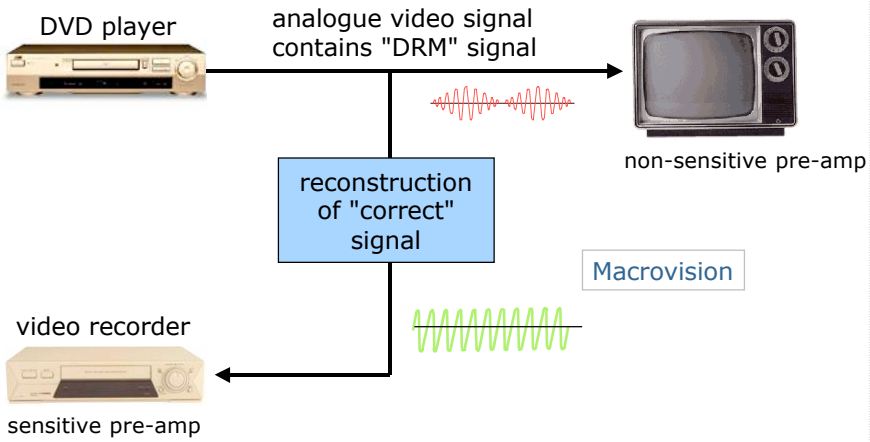
- Schlüssel ist im Abspielgerät
  - Abspielgerät entschlüsselt
  - Player gibt die Inhalte in niedriger Qualität aus




IT-Sicherheitsmanagement
Prof. Dr.-Ing. Hannes Federrath

## Fall 2: Verschlüsselter Inhalt auf Datenträger

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



## Fall 2: Verschlüsselter Inhalt auf Datenträger

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

DVD player

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

IT-Sicherheitsmanagement
Prof. Dr.-Ing. Hannes Federrath

## 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
- 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)

## Zwischenfazit

- 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

- 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
  - 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

## 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

IT-Sicherheitsmanagement
Prof. Dr.-Ing. Hannes Federrath

## 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

## 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

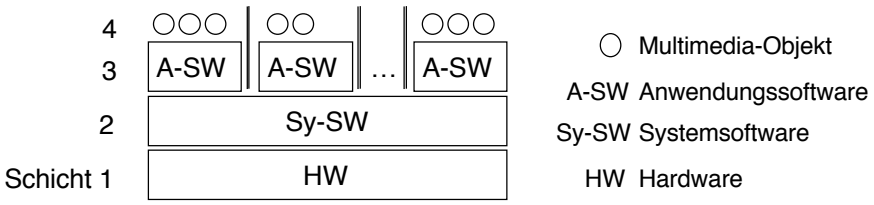
IT-Sicherheitsmanagement
Prof. Dr.-Ing. Hannes Federrath

## Fall 4: Verschlüsselter Inhalt

- 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

- 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.




IT-Sicherheitsmanagement
Prof. Dr.-Ing. Hannes Federrath

## 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

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

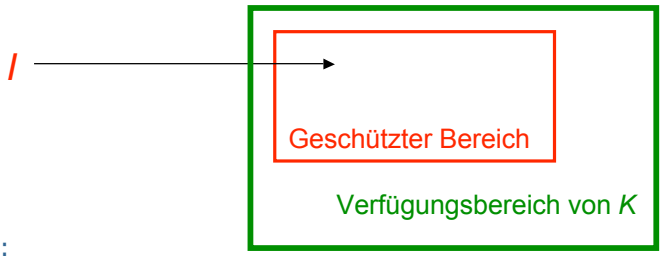


## Nicht frei programmierbarer Universal-PC

- 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

## Fazit

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




- Ergebnis:
  - Sowohl Offline als auch Online sind — mit wissenschaftlichen Maßstäben gemessen — keine Techniken in Sicht, die einen technischen Urheberschutz zuverlässig gewährleisten, solange es frei programmierbare Multimedia-Computer gibt
  - Die meisten Techniken erschweren zwar das digitale Kopieren und die Nutzungserweiterung, verhindern sie aber nicht.