Wissenschaftliche Bewertung von DRM-Systemen

Scientific evaluation of DRM systems

Hannes Federrath

http://www.inf.tu-dresden.de/~hf2/

- Adversary model
- Strength of existing systems
- Tendencies
- DRM technologies
- Summary

core.ac.uk metadata, citation and similar papers at core.ac.uk
brought to you by CORE
provided by University of Regensburg Publication Server

What is the scope of the attacker?

- More general: What are the security demands?
  - confidentiality of content
  - integrity of content
  - availability of content

- Confidentiality:
  - protection against piracy
    - copy one content
    - copy every content in a certain time frame
    - break the entire system (copy every message at every time)
- Integrity:
  - authorized access to content
  - protection of ownership of content
- Availability:
  - prevention of denial of service attacks

Adversary model

- Security depends on the supposed strength of the attacker.

- Resources
  - Money
  - Time
  - Knowledge
- insider or outsider
  - concerning organizational aspects (secrecy of master encryption keys)
  - concerning design secrets (e.g. of protection functionality in hard- and software)
- Who wants to attack a system?
  - Hobbyist (naïve attacker, no financial efforts)
  - Serious attacker (intelligent, probably no financial efforts)
  - Professional attacker (intelligent, financial motivation)

The existence of specialized tools shifts the "knowledge" to anybody

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

Tendencies

- Pirates try to “reverse engineer” DRM systems
  - make them useable on other platforms (Linux, …)
  - make them independent of a certain hardware and software seller
- Pirates in the Internet shift their “activities” to services
  - peer-to-peer services
  - anonymous communication services
- Pirates may use Trojan Horses to get content illegally
  - This is a very subtle and serious thread!
- Attackers make their knowledge public as automated tools
  - Hobbyists can now do professional attacks

DRM Technologies

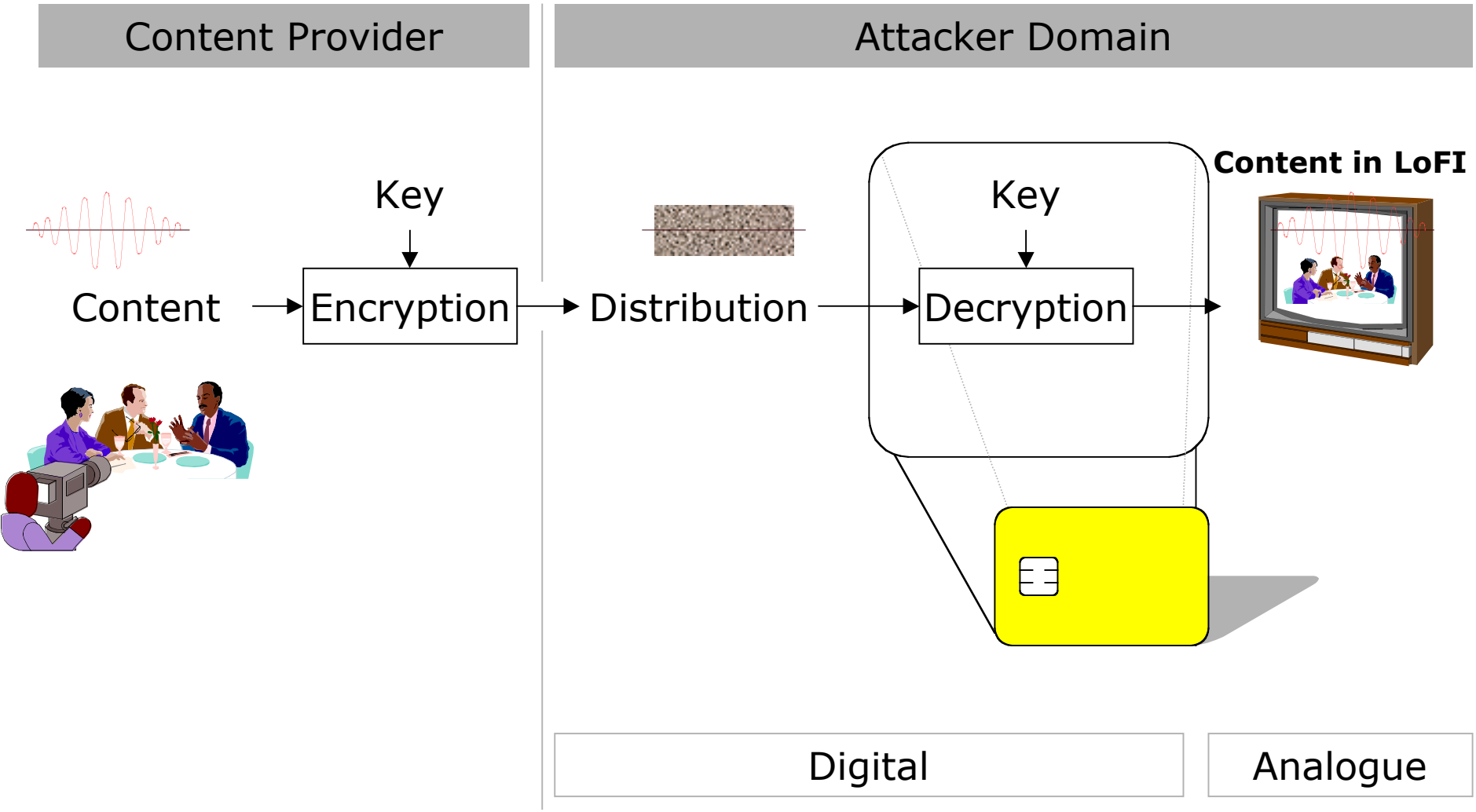
- Basic IT security technologies
  - Encryption
  - Tamper resistant hardware devices
- Special designed DRM technologies
  - Fingerprinting
  - Watermarking
- Naïve security mechanisms
  - Regional coding of content
  - Filter mechanisms
  - Incompatible formats and media
  - DRM codes without any protections against removing
  - ...

content detection

copy protection

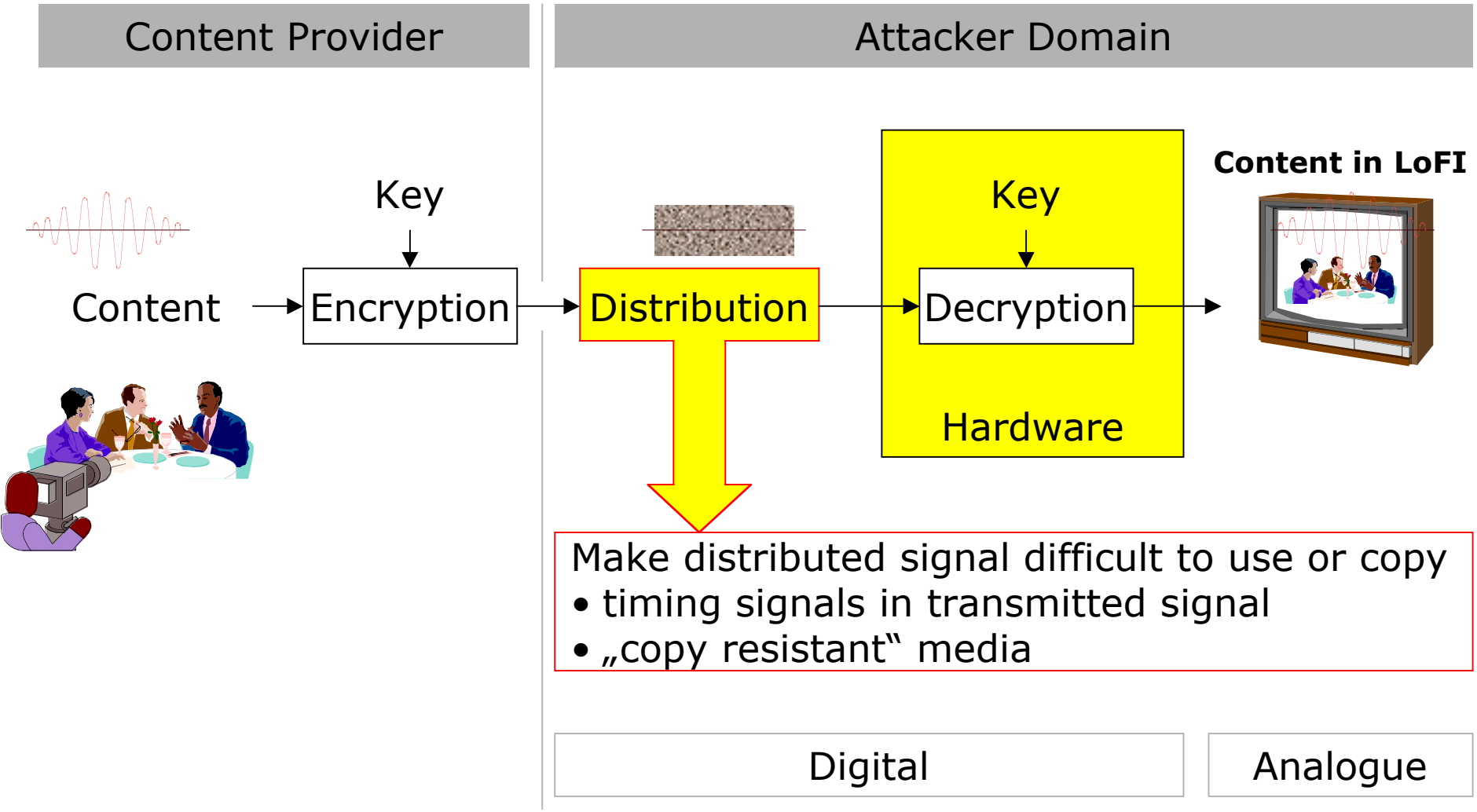
Design Options for Copy Protection

⌘ Protect pay-services from unauthorized access

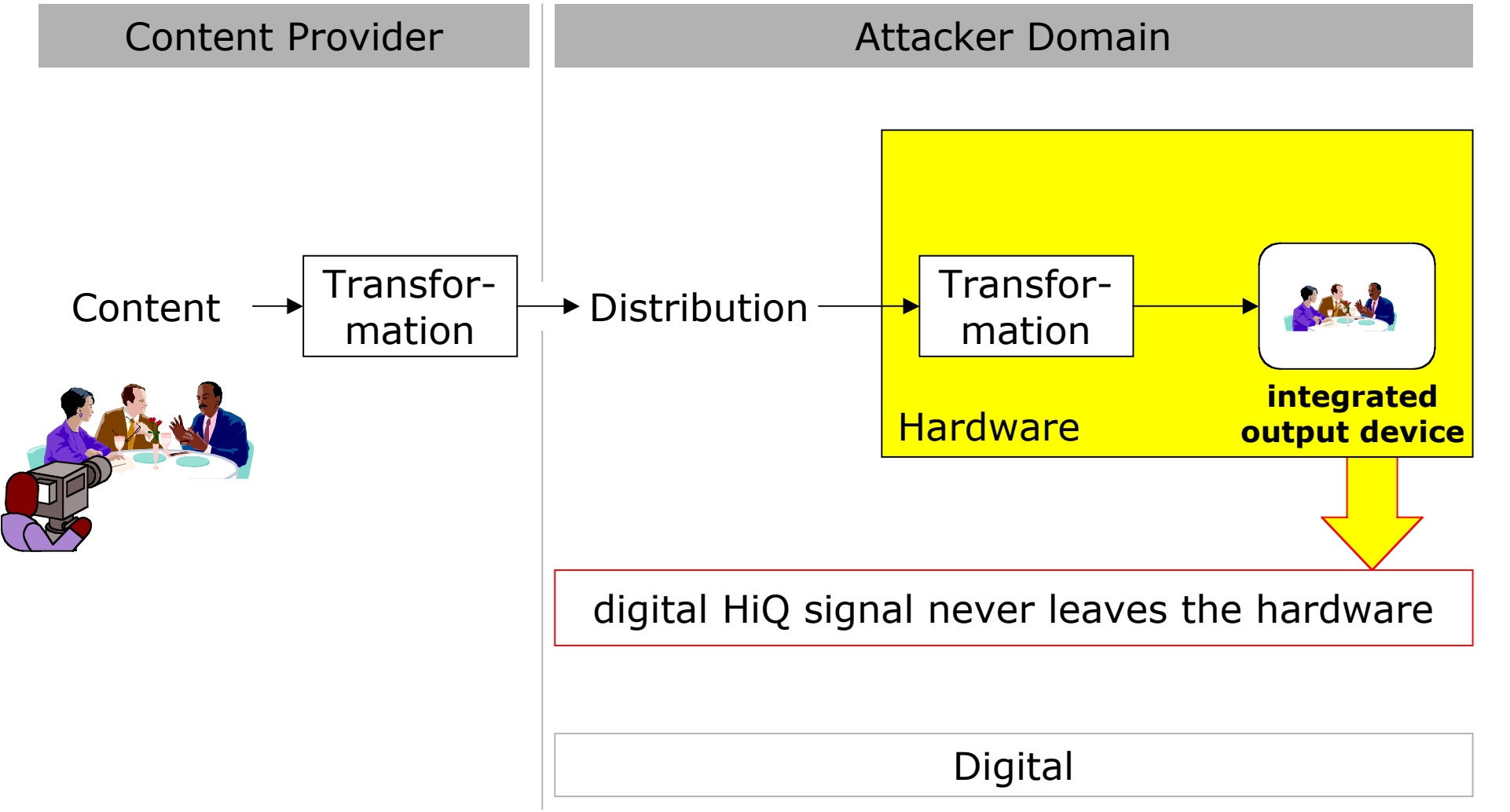


Design Options for Copy Protection

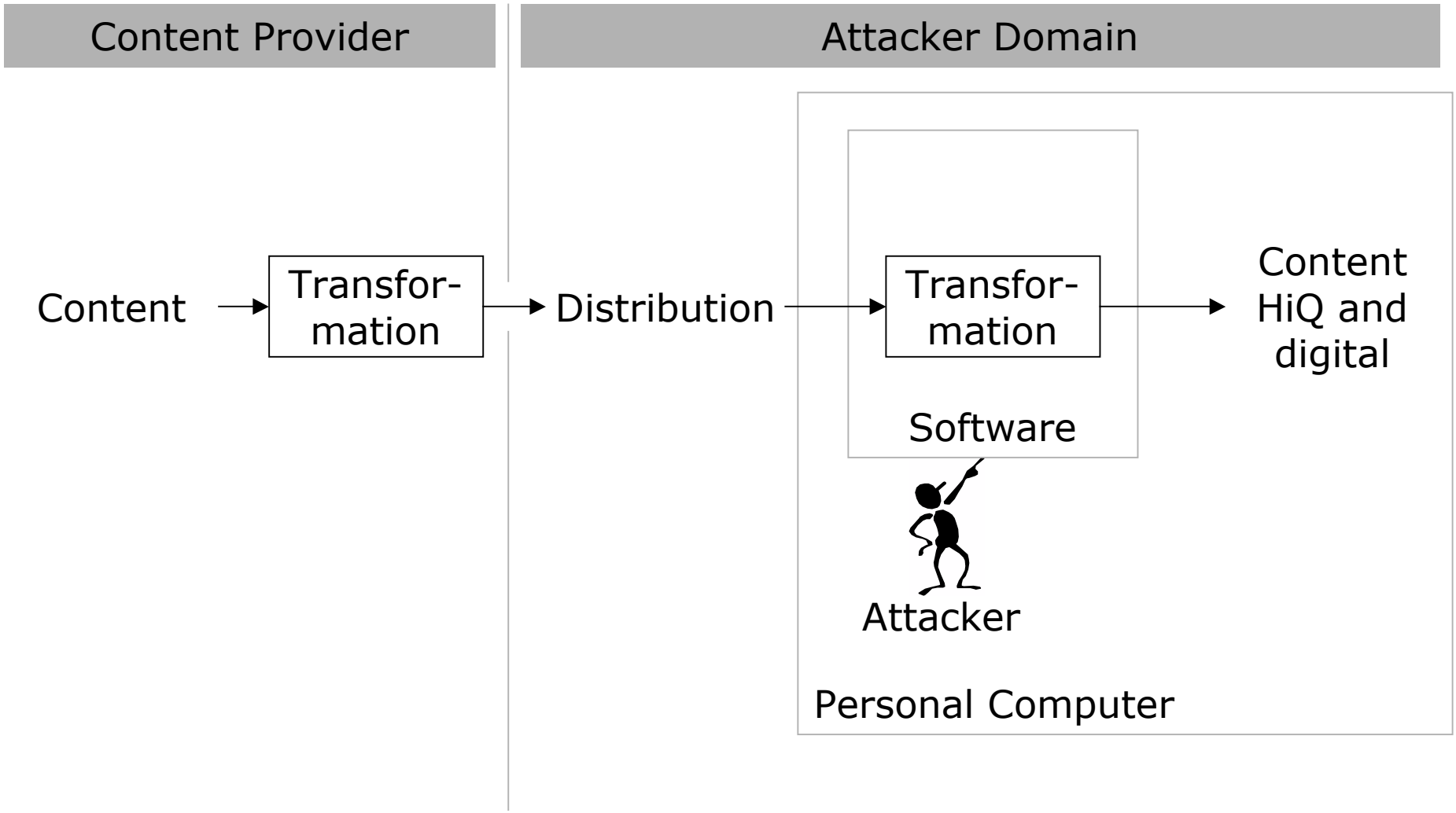
⌘ Protect pay-services from unauthorized access



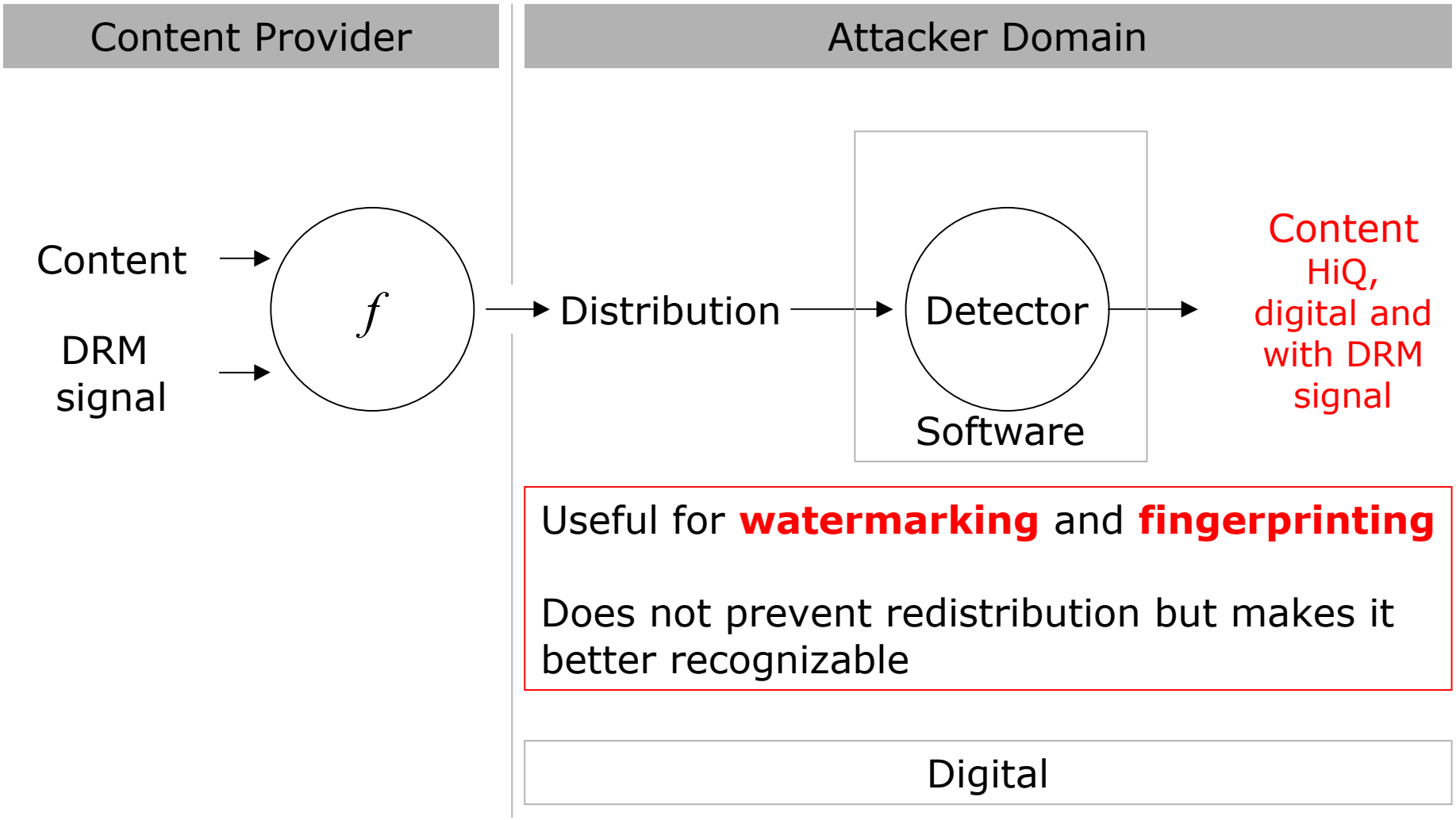
Design Options for Copy Protection



Never! Too dangerous!



What is possible in software?



What is possible in software?

Content Provider	Attacker Domain

Attention!

Scope is changing!

Not: Protection against illegal copying

But: **Detection** of copies

Cont

DRM
sign

Content
HiQ,
igital and
with DRM
signal

printing

Does not prevent redistribution but makes it better recognizable

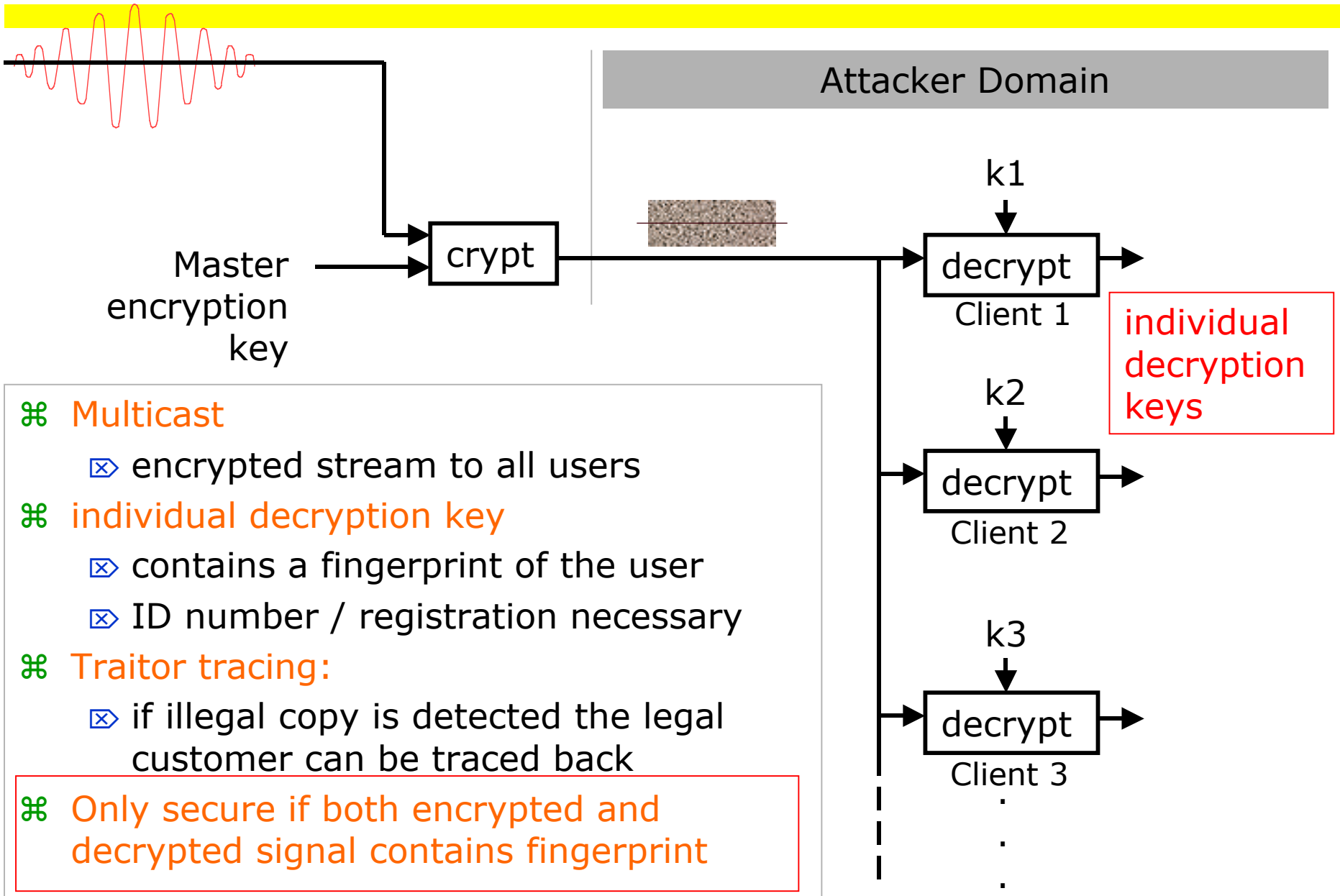
Digital

DRM Technologies

- Basic IT security technologies
  - Encryption
  - Tamper resistant hardware devices
- Special designed DRM technologies
  - Fingerprinting
  - Watermarking
- Naïve security mechanisms
  - Regional coding of content
  - Filter mechanisms
  - Incompatible formats and media
  - DRM codes without any protections against removing
  - …

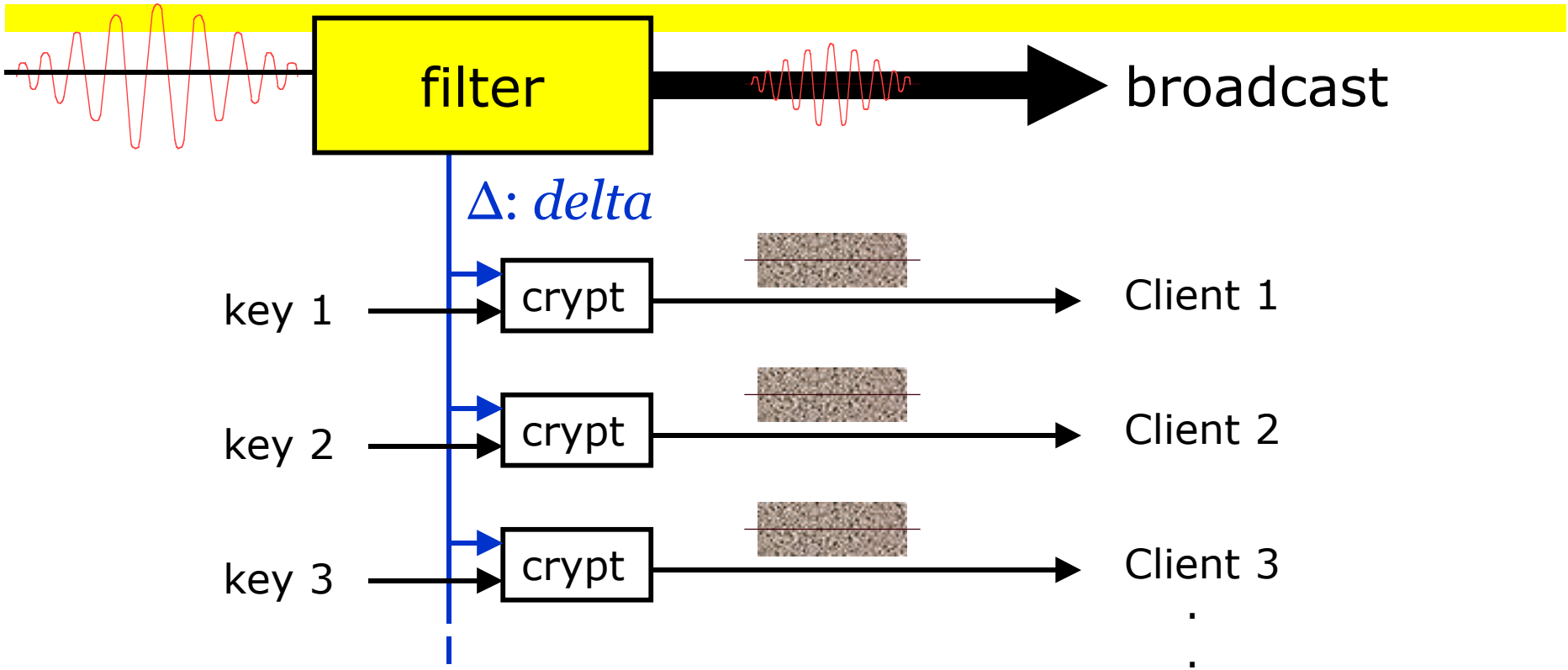
content detection

Broadcast encryption



- Multicast
  - encrypted stream to all users
- individual decryption key
  - contains a fingerprint of the user
  - ID number / registration necessary
- Traitor tracing:
  - if illegal copy is detected the legal customer can be traced back
- Only secure if both encrypted and decrypted signal contains fingerprint

> LoFi Broadcast, HiFi Encryption



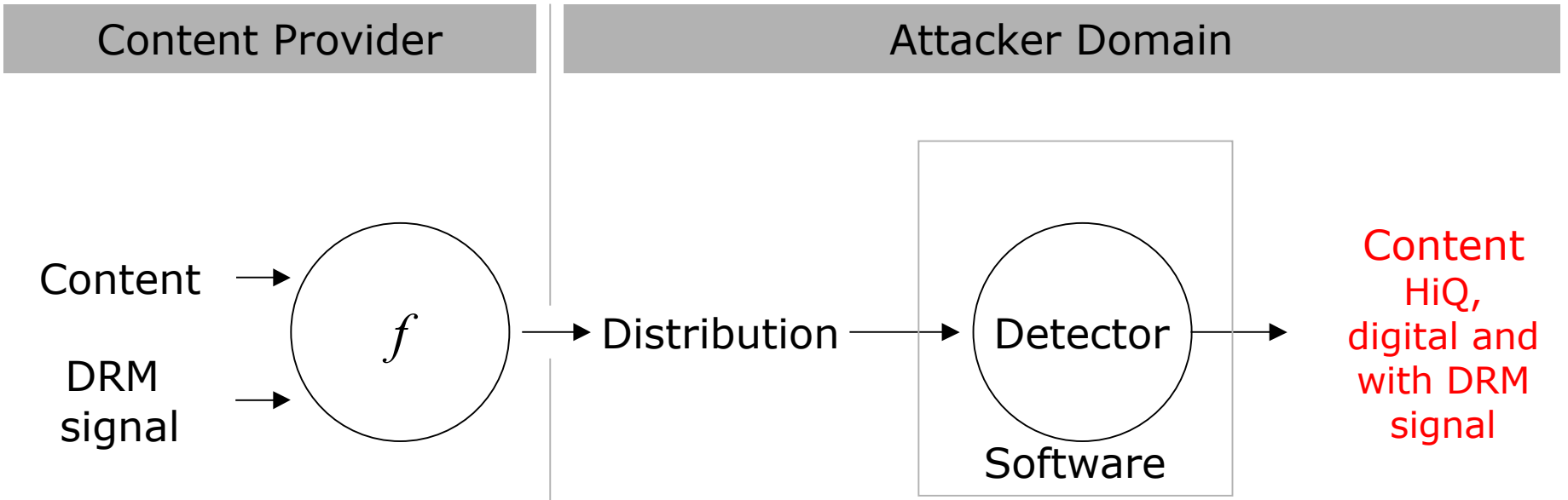
- Divide stream into quality layers
  - Everybody gets the low quality layer
  - Paying customers get encrypted layers
- MP3:
  - division of mp3 stream into quality layers
- costs are linear in the number of users

DRM Technologies

- Basic IT security technologies
  - Encryption
  - Tamper resistant hardware devices
- Special designed DRM technologies
  - Fingerprinting
  - Watermarking
- Naïve security mechanisms
  - Regional coding of content
  - Filter mechanisms
  - Incompatible formats and media
  - DRM codes without any protections against removing
  - …

content detection

Watermarking



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

Digital

Watermarking

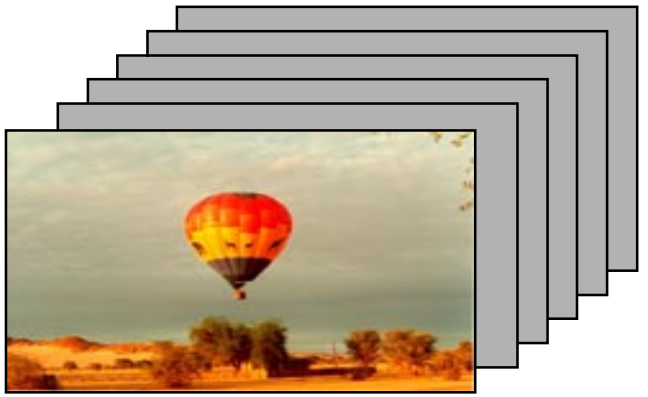
- Scope: Protect authorship of digital content
- correlation necessary
- few 100 bit
- strong changes

Original

Key

Embedding

Distribution



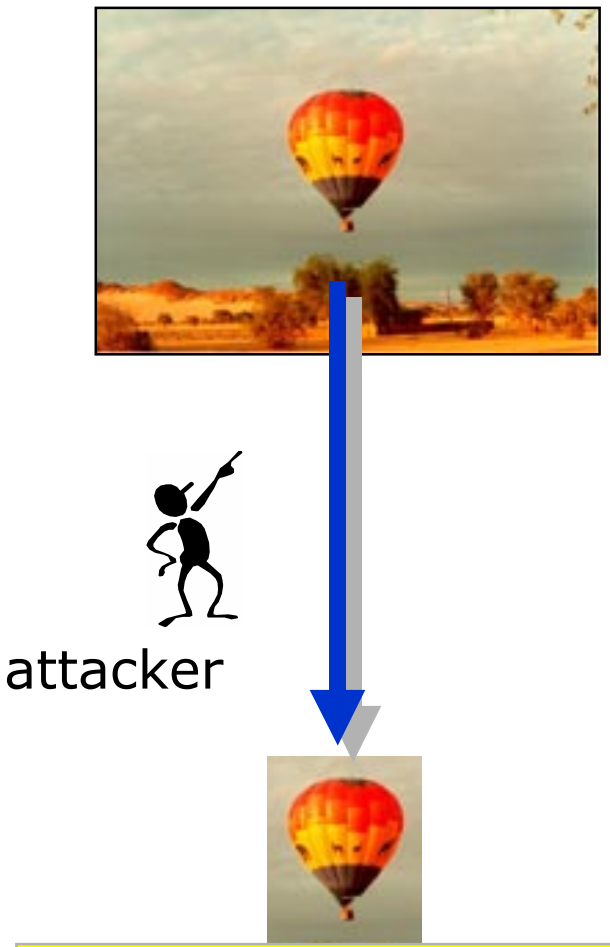
Attacker

Watermark Signal:

Copyright (C) 1998
Document-ID: #A53-229D789
Author: J.Fitzgerald
Title: White Christmas

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

- ⌘ Collusion Attacks



Copyright (C) 1998
Document-ID: #A53-229D789
Author: J.Fitzgerald
Title: White Christmas

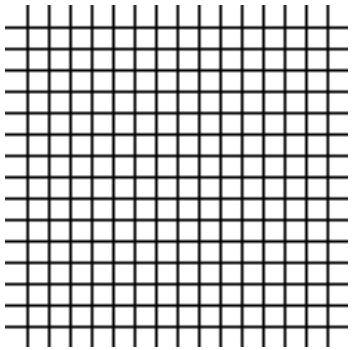
> Security of watermarking systems

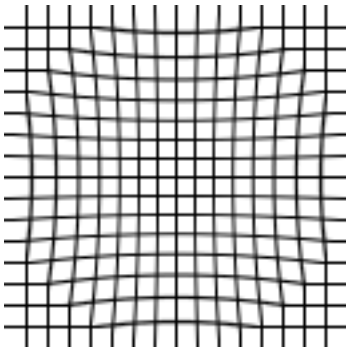
- Theory
  - robustness
  - non-interference
  - detectability

- 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

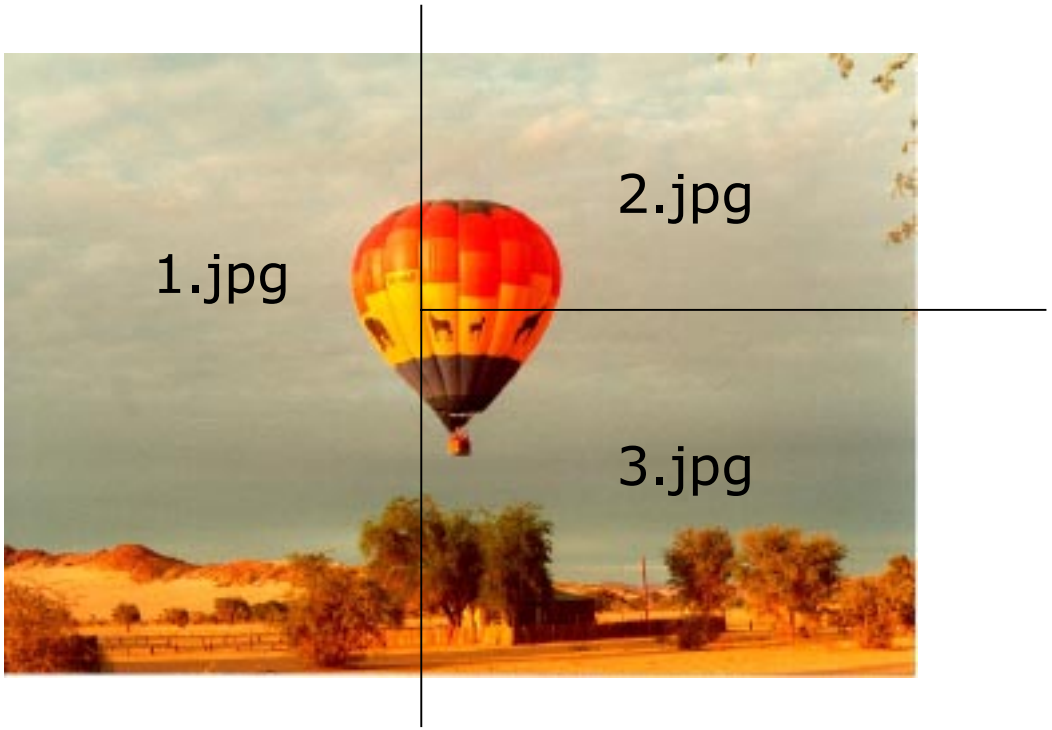
- non-linear transformation of a picture
- synchronization gets lost
- no anchor for detector to find the position of embedded signal





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

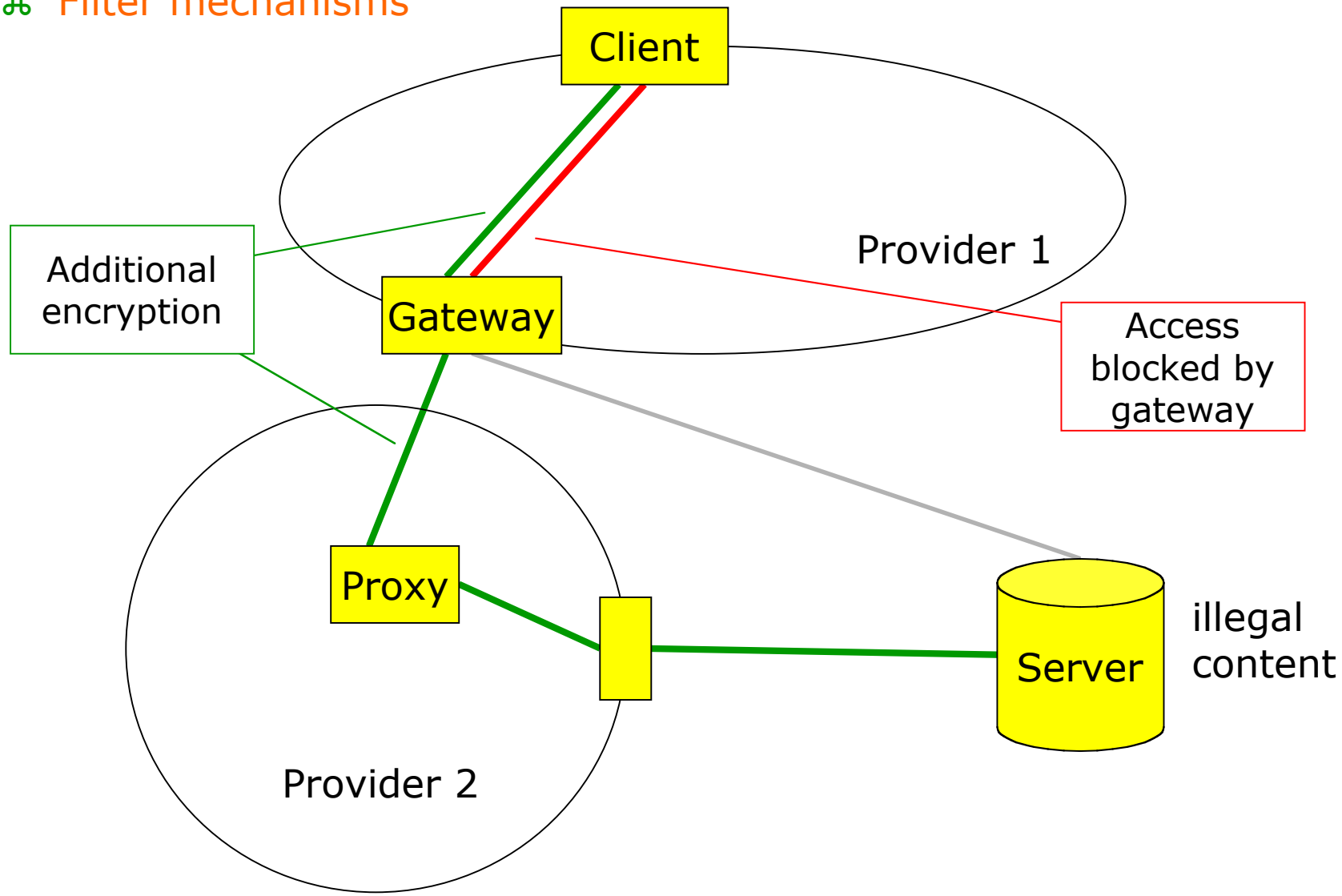


DRM Technologies

- Basic IT security technologies
  - Encryption
  - Tamper resistant hardware devices
- Special designed DRM technologies
  - Fingerprinting
  - Watermarking
- Naïve security mechanisms
  - Regional coding of content
  - Filter mechanisms
  - Incompatible formats and media
  - DRM codes without any protections against removing
  - ...

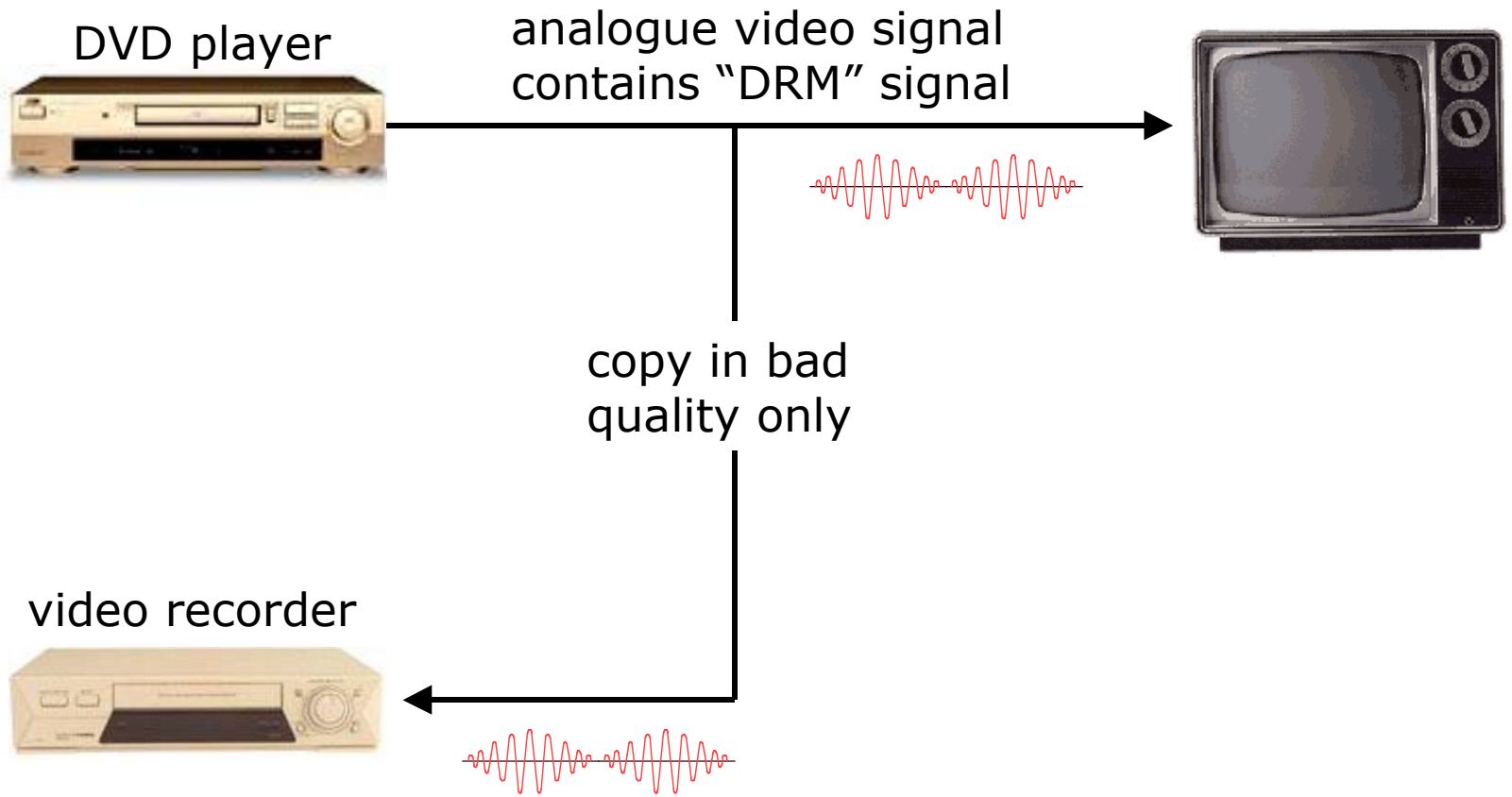
Naïve security mechanisms – examples

⌘ Filter mechanisms



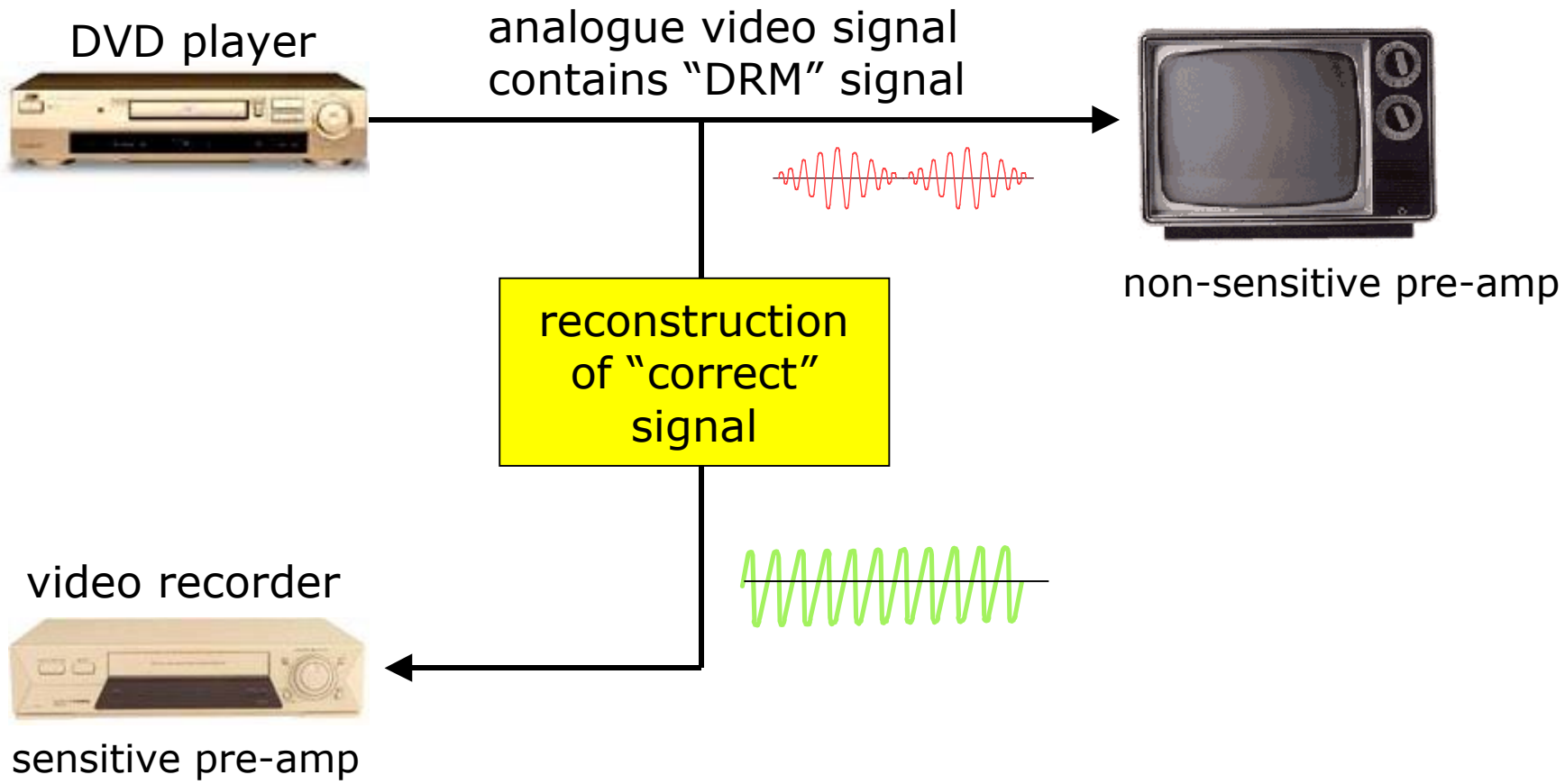
Naïve security mechanisms – examples

- copy protection in videos recorders



Naïve security mechanisms – examples

- copy protection in videos recorders



Naïve security mechanisms – examples

- DRM codes without any protections against removing

digital audio player

digital audio

digital recorder

MD, CD-R (Audio), DAT

Original: copy bit unset

0100101011101011101010011100110010

Copy: content with copy bit set

0100111011111011111010110111011100 11

Naïve security mechanisms – examples

⌘ DRM codes without any protections against removing

digital audio player

digital audio

digital recorder

MD, CD-R (Audio), DAT

Original 0100101011101011101010011100110010

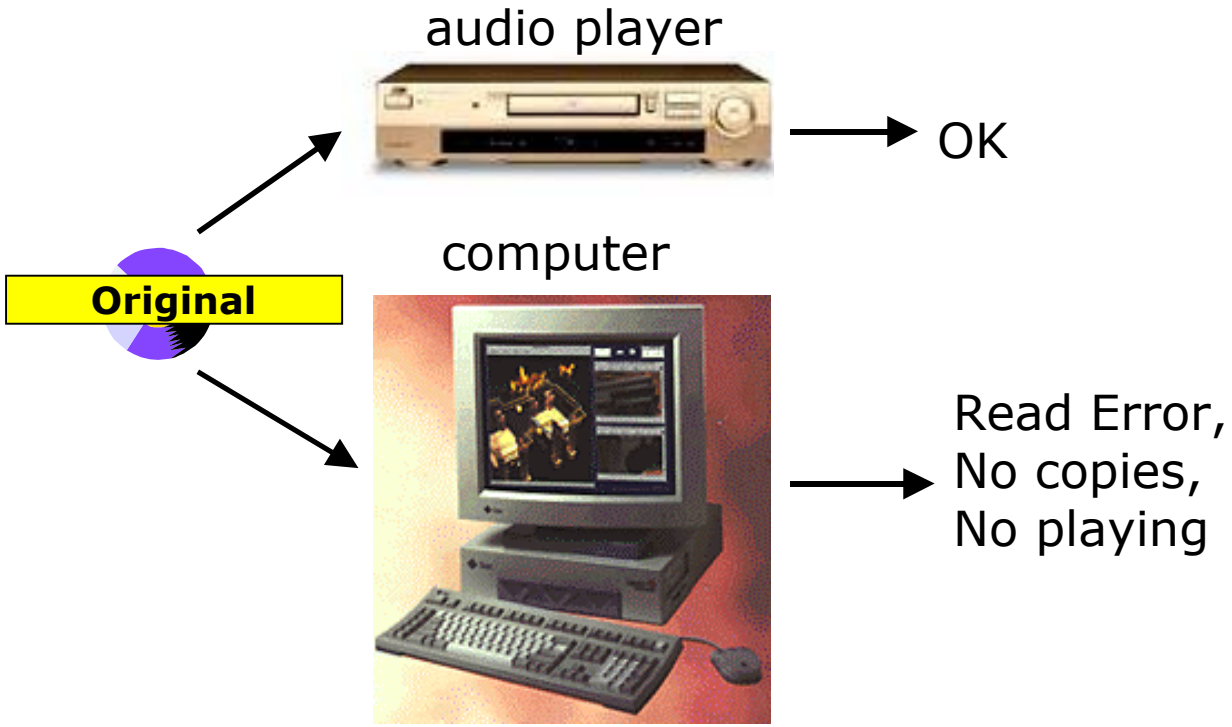
Copy 0100111011111011111010110111011100 11

Reset copy bit to make copies

Copy 010011101111 [ ] 010010101110 !

Naïve security mechanisms – examples

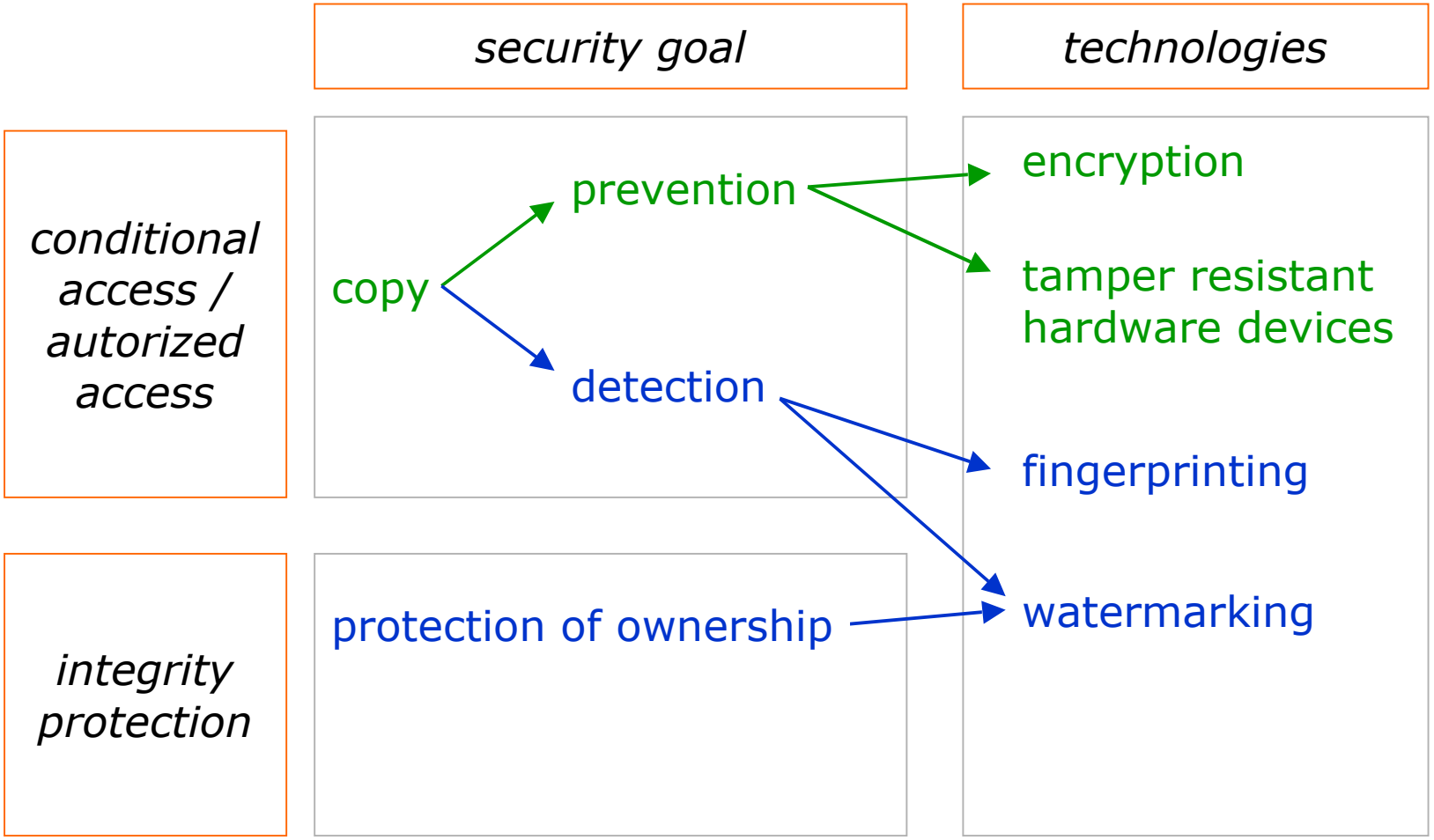
- incompatible formats and media



Naïve security mechanisms – examples

- incompatible formats and media

Basic security goals and corresponding technologies



Secure DRM systems

- Secure DRM systems connect a DRM signal with the content to protect in a way that the content signal is useless without the DRM signal.

- Options:
  - DRM signal is part of the content signal (e.g. in watermarking systems)
  - DRM signal is necessary to access/decrypt the encrypted content signal
- Important point:
  - Detection of DRM signal cannot be bypassed
  - Hardware or software encapsulation

- Software
  - not recommendable
- Hardware
  - breaking is a matter of time and money