

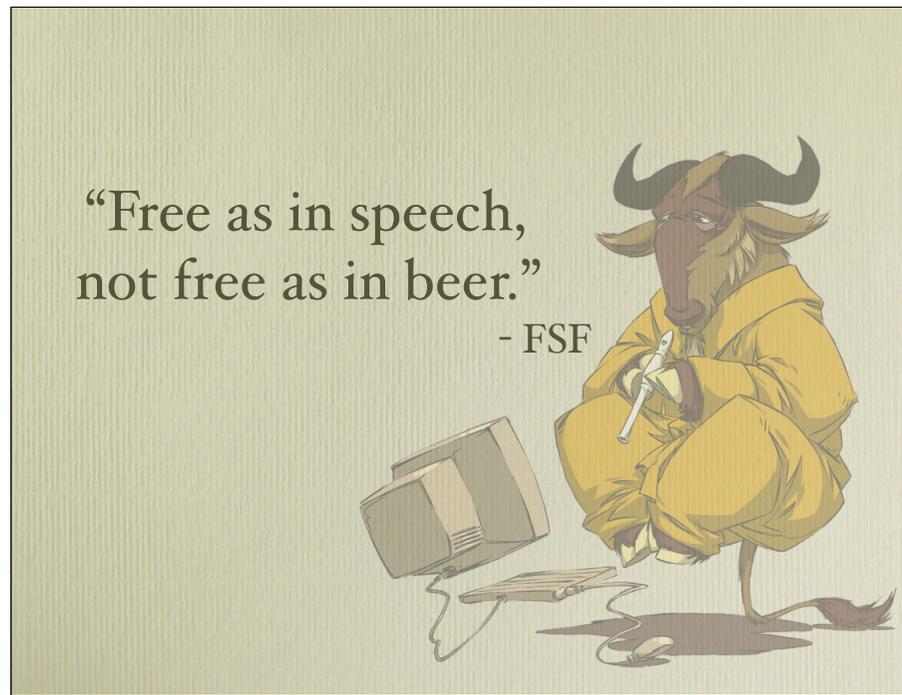
- overview
  - What's the motivation behind DRM?
  - How does it work?
- start off with a view on the way our culture gets made
- Lawrence Lessig wrote: "Code and other laws of the Internet", "Free Culture"
- he observed: The way our culture gets made is changing from a free culture to a permission culture
  - and summed it up

“If we understood this  
change, I believe we would  
resist it.”

- Lawrence Lessig



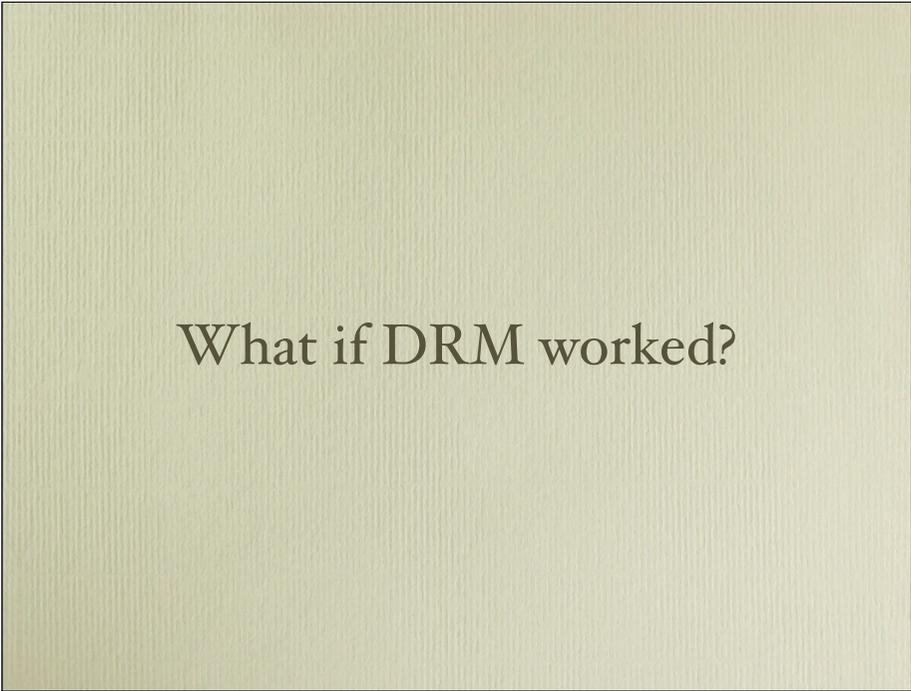
- culture == content
- he founded the creative commons as a means of resistance
- What does he mean by this?



- Free Culture is:
  - free markets, free trade, free enterprise, free election
  - not a culture without property, just as in a free market not everything is free
  - supports and protects creators and innovators
    - directly by granting intellectual property rights
    - indirectly by limiting those rights so that follow up creators remain as free as possible from control of the past
- > standing on the shoulders of giants



- Permission Culture
  - the opposite of a free culture
  - creators create only with the permission of the powerful
  - or the creators of the past
- you have to be on the lookout not to collide with their "rights" / monopolies
  - quite hard to detect -> "Free Culture" has more about this
- just two examples of consortiums that seem to stand for a permission culture
  - Recording Industry Association of America
  - motion picture association of america
  - they think that (compulsory) DRM helps their business



What if DRM worked?

- lets assume that:
  - if it is reasonably hard to crack
  - than to find something on polluted file sharing networks
  - to ordinary customers who find it more convenient to buy

## Some new business models?

- Club / Subscription
- Renting Content
- Pay per view

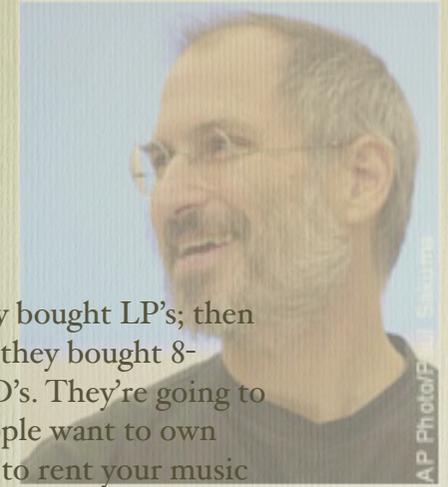


- so this is what you want as a publisher
  - club, abo
    - jamba, ringtones -> first ringtone gives you a subscription
    - bertelsman / weltbild / newspaper
  - renting music: video rentals, libraries
  - pay per view: TV, jukeboxes
- attacked by pirates, but if they are out = business is easy this way
  - lock in / cost of change -> especially renting
- they are so similar to the old models

but...

“They bought 45’s; then they bought LP’s; then they bought cassettes; then they bought 8-tracks; then they bought CD’s. They’re going to want to buy downloads. People want to own their music. You don’t want to rent your music -- and then, one day, if you stop paying, all your music goes away.”

- Steve Jobs, Rolling Stone interview



- he says about customers
- the ITMS proves him right (today)
- failed CD copy-protection
- customers don't want it
- business on the other hand

## DRM though enables ...

- to control who creates
- to control markets



Quelle: airporttechnology.com

Quelle: htmramp.com

- so this is what you want as a publisher
  - first of all you get to control who uses your content to create new content
    - "standing on the shoulders of giants"
- there is a fear that this will cement old business models / monopolies
  - and bring less competition, new monopolies (in the content industry)
  - apples fairplay is a good example of this: they keep competitors out of the ipod
- So, how does this work?

# How does DRM work?

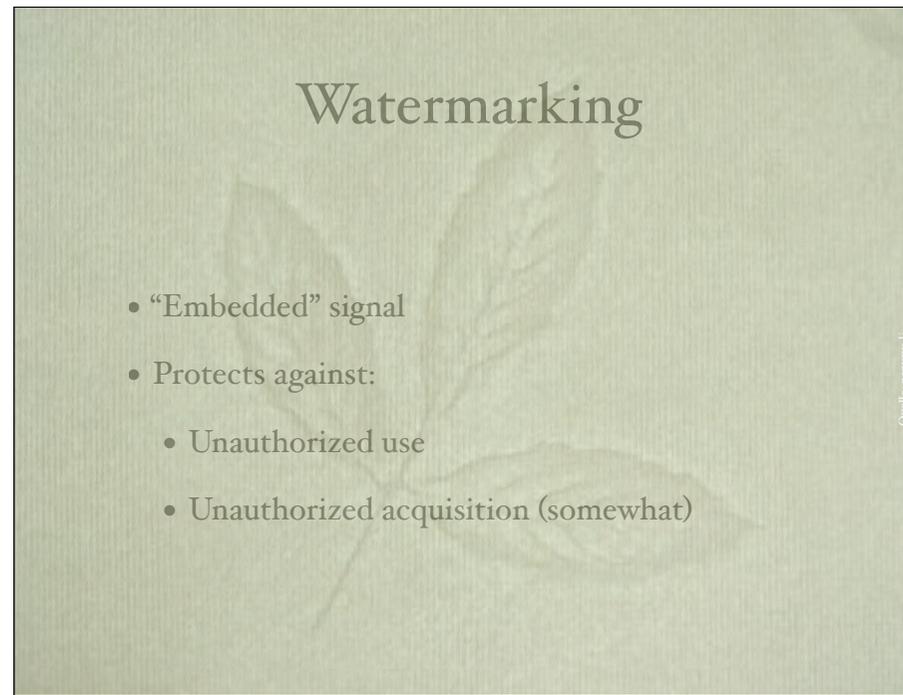
- Unauthorized use and acquisition
- Three approaches
  - Watermarking
  - Fuzzy hashing
  - Secure containers



Quelle: ibid. gbk.com

Quelle: apple.com

Quelle: tempus.at



- relies on the "bad" theory of human perception
  - leftover bandwidth is used
- attacked by:
  - digital -> analog (the analog hole) -> could survive that
  - scaling, re-compression-> possible to survive that
- therefore cannot be strongly assessed
  - though empirically it is proven that removing the watermark degrades the signal
- unauthorized use: ok
- unauthorized acquisition: if detectors are widely spread
  - though needs constant internet connection or big database (how to update?)

# Fuzzy Hashing

- The content becomes the hash
- Protects against:
  - Unauthorized use
  - Unauthorized acquisition (somewhat)

Hash Table(strings)	
0	(null)
1	(null)
2	(null)
3	"Steve"
4	(null)
5	(null)
6	(null)
7	(null)
8	(null)
9	(null)
10	(null)
11	(null)

© 2011, p4pp0n4, ll

- relatively new
- the content becomes the watermark
- also relies on the human perception model
  - everything that is perceived the same gets the same hash
    - bit-flipping won't change it
- attacked by:
  - modifying the content so the hash changes
    - won't work if the human perception model is good
    - or at least would degrade quality (more if the model is good)
- unknown robustness (too new)
  - needs to be very precise, almost no false positives
  - public or business content that doesn't render := catastrophe
- use and acquisition -> same as with watermarking

## Secure Containers

- Encrypting the content
- Protects against:
  - Unauthorized use only

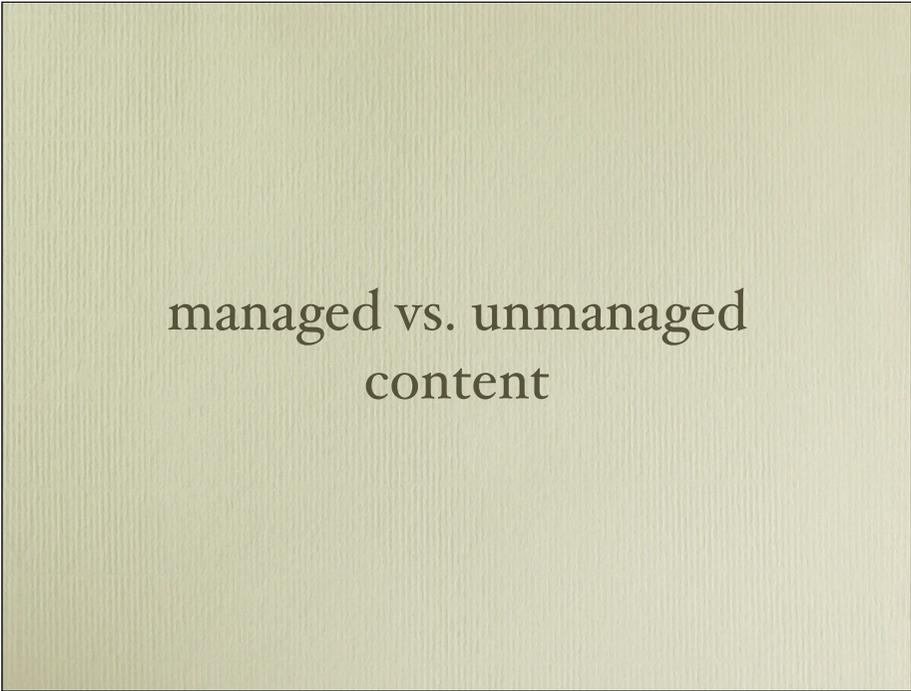


- encrypting content
  - problem is shifted to managing keys
  - user needs access, but is not "trusted"
    - Trusted Platform comes in right here
- great at targeting specific users, devices
- no eavesdropping during the transmission
- attacked by:
  - tricking the license evaluating engine into releasing the content
  - attacking device drivers
  - hacking the TPM (virtual machines, hardware, TODO?)
  - analog hole
    - most "easily" broken by determined adversaries?
- robustness: as good as the TCB below it is
- unauthorized use: jup
- unauthorized acquisition: not dealt with by this

“We claim [...] this would  
have little effect on piracy.”

- S. Haber, B. Horne, J. Pato, T. Sander, R. E. Tarjan

- no perfect technique
  - but could possibly made secure enough to stop all the but the most determined adversaries
- watermarking & fuzzy hashing also deal with unauthorized acquisition
- but it would need a standard system, that is deployed ubiquitously
- would that stop piracy?
  - "Pick one lock -- open every door." - Steve Jobs, Rolling Stone interview
  - "unmanaged-content" has to be rendered ????
  - distribution via the "darknet" is very efficient



managed vs. unmanaged  
content

- I'll have to rehash a concept from those guys
  - managed vs. unmanaged content
- problem: unmanaged content
- if unmanaged problem is the problem, then having only managed content could be the answer
  - this is what they call: "Draconian Content Management"



- the solution would be to only handle "managed content"
  - which can only be played by trusted software/systems
  - with secure output channels (microsoft anyone?)
- since by definition there is now no unmanaged content
  - there is also no possibility for unauthorized use
  - and therefore unauthorized acquisition is no problem too
- but...

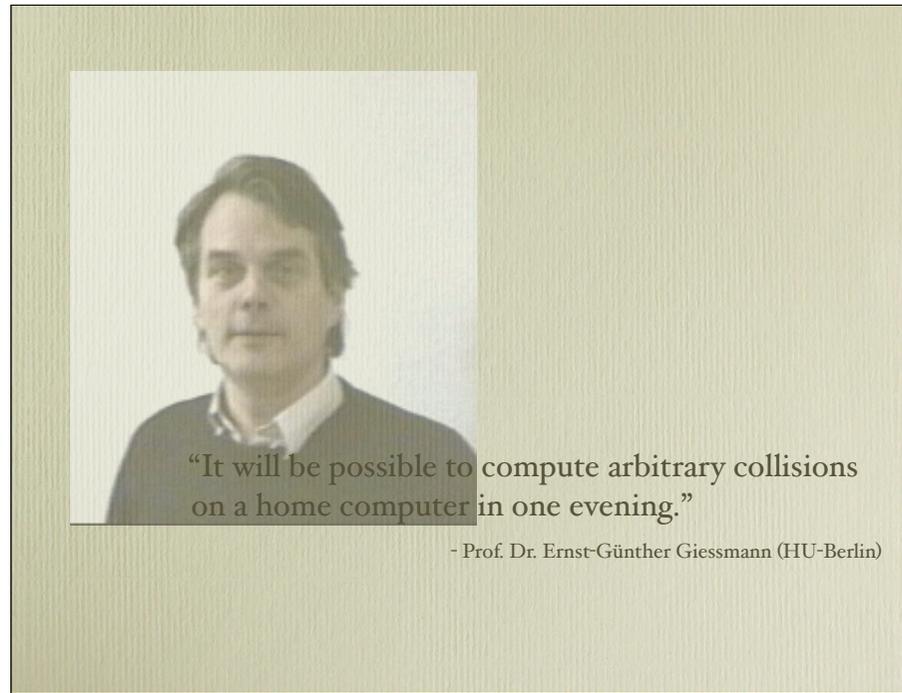
## Some Problems

- New devices
- License authority
- Public content
- Private content

TOP  
SECRET

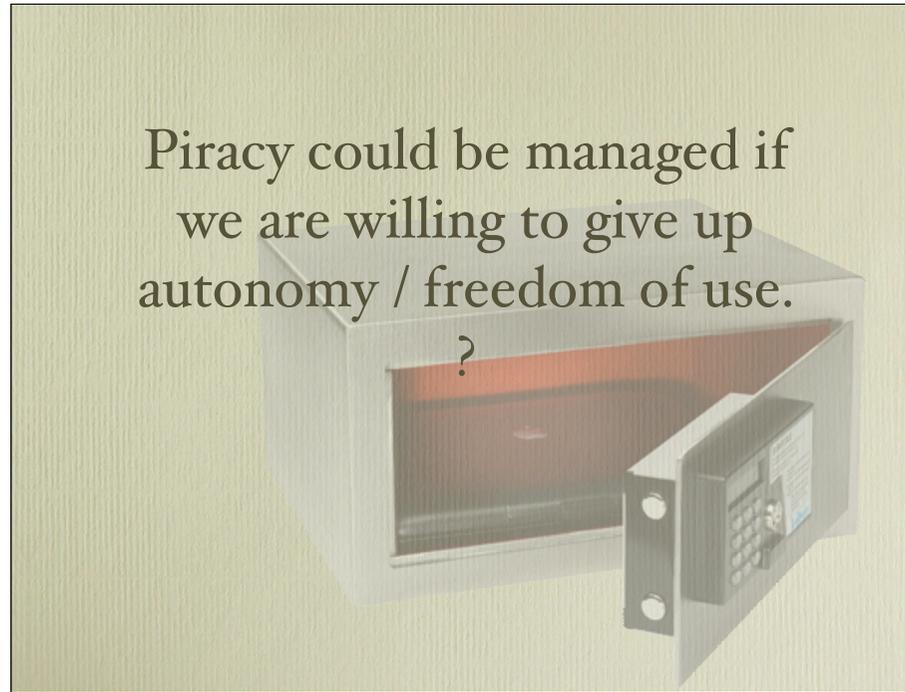
XXX?

- some problems:
  - completely new device infrastructure needed
  - what about public content
  - who issues licenses (for public content?)
    - central authority?
    - decentralized (recording devices) -> database problem again
  - and content people don't allow/want to have a license?
    - private content, business correspondence, classified content?
    - maybe you don't want to certify your private pornography?
- not feasible....
- so parallel infrastructure for unmanaged content is a must
  - > which breaks draconian DRM
  - though draconian DRM could try add value
    - better quality, lower cost
    - vendors could do the same for untrusted systems
- technical foundation of TPM is hashing, but....



- all of the TPM is based on strong cryptographic hash-functions
- but they are basically broken by now
- just last week cryptographer Prof. Dr. Ernst-Günther Giessmann (HU-Berlin) was quoted that SHA1 will be completely broken by the end of the year. (at least so he says)
  - Compute the difference needed between a freebsd hash and a windows hash
    - pad the freebsd and boot it instead of windows
    - then use it to rip of all the movies you downloaded with windows
  - BORE
    - Broken Once (re-encoded) and Run Everywhere
- no different hashing algorithms to work with
  - arms race

Piracy could be managed if  
we are willing to give up  
autonomy / freedom of use.



- Where does this end?
  - Completely tamper resistant hardware
  - nobody knows what's going on inside
  - you get your own crypted content
  - security by obscurity?
- 
- Nikolaus is going to say more about this
- 
- sum it up

## Not Feasible:

- Technically
- Economically
- Socially



Quelle: weknow.com

- so it is technically not feasible
- economically we are not sure
  - completely new hardware for every customer -> will they do it? (CD copy protection had problems)
  - does fighting piracy even refund?
  - new monopolies might arise
- socially there are quite some changes to the way we make and perceive culture
- this is what Lessig meant when he said...



“... we would resist it!”

- Lessig

Quelle: [www.lessig.org](http://www.lessig.org)

- just switch over to the next slide
  - What could we do then?

## What could we do then?

- if the systems are reasonably hard to break
- file sharing systems have lots of spam, spyware
- and some users are prosecuted quite publicly for sharing
- it could be much more convenient just to buy the stuff in a good online store
  - ITMS?
- so we should
  - Preserve the free culture (there's a reason it was created)
  - maybe Compete with it?

## Is competing possible?

- 40% of all software is pirated
- Solarium vs. self tanner vs. sunbathing
- Water bottlers vs. city waterworks



- Competition against free (or low cost) is possible
- flat rates could stimulate usage, instead of “milking” customers with subscriptions
- Yes it is possible
- Here’s how!

## Here's how!

- Content management
- Content delivery
- Business models



Quelle: ibiconsulting.de/Int



Quelle: pary-rhodan.net

- good content management: recommendations (ITMS) / organization
- content delivery:
  - fast downloads
  - good quality
    - "darknet"/file sharing networks often have minor quality, spam,...
  - infrastructure: cheap and easy access from everywhere (e.g. mobile phones?)
    - mobile phones is a walled garden: pirates cannot do that
- business models:
  - alternative ways of charging for access
    - subscription / flat-rate / bundling / price discrimination
      - discrimination of risk of pirating (depending on format)
  - linking different offerings: concert tickets, clothing, club membership, construction kit...
- Summary
  - eliminate piracy by technical means is impossible
  - most of these are things, no pirate can/could offer

thanks, questions, is it possible to compete?