A BRIEF HISTORY OF ANTI-PIRACY

OVERVIEW

The non-naval kind

Glossary

- The following will be used interchangeably:
  - *Copy protection/prevention*
  - *Digital Rights Management (DRM)*
  - *Anti-piracy measures*

WHAT IS A PIRATE?

- The people that create illicit copies of media
- The people that distribute that media
- The people that consume that media

A STORY AS OLD AS...

570 AD

WE WILL NOW LEAVE BEHIND ANY DISCUSSIONS ON HOW GOOD/BAD DRM IS

Else this will surely become a two hour rant.

And I’m not drunk

yet

AIMS OF ANTI-PIRACY

Make it difficult to make unauthorized copies

Traitor tracing

Revocation of access

Unobtrusive to legitimate usage

CONTENTS

- General Techniques
  - Watermarking and Steganography
  - Cutting off supply
  - Source-to-sink protection
  - Online verification
  - Anti reverse engineering
- Specifics
  - Cinavia
  - HDCP
  - AACS
  - Widevine
  - VMProtect
  - Miscellaneous

WATERMARKING AND STEGANOGRAPHY

Overt watermarking

Hard subbing

Steganography

Mick Gordon. “Doom: Behind the music”, GDC 2017
https://www.youtube.com/watch?v=U4FNBMZsqrY

Printers and their sneaky yellow dots

- Anti-money counterfeiting measure
- Devices will print a small arrangement of yellow dots on any sheets printed
  - *Hardly perceptible unless you know it'll be there*
- Each pattern uniquely identifies a machine and includes a timestamp.

Why?

- Identification of sources
  - *A broadcaster*
  - *A reviewer / beta tester*
- Can help categorize the leaker.
  - *Eg/“All the camrips come from ‘Odeon’+‘North England’ screenings”*

Mitigations

- Produce poor quality replicas
  - *A high contrast, black and white scan of the documents will obliterate the yellow dots*
- Source mixing
  - *An average of a number of sources will muddle the watermarks*
- Watermark removal techniques
  - *If you know where to look, obfuscate or remove only those parts*

CUT OFF THE WATER HOLE

DMCAs, Raids and other legal action

- A “Digitial Millenium Copy Act” notice can be served to ask people to remove links to pirated material.
- Site takedowns (Napster, KAT, Alphabay)

Blacklisting of certain domains

- ISP level blocking of access to certain domains and/or IPs
  - *PirateBay.<xy/se/eu>, kat.<cr/it/se>, nyaa.<eu/se>*
- Search engines and DMCA's
  - *Request removal of results from search engines*

Tracking of network usage

- High upload from “home” user
- Protocol tracking
- Unusual times of operation
  - *Most home users aren’t online 24/7*

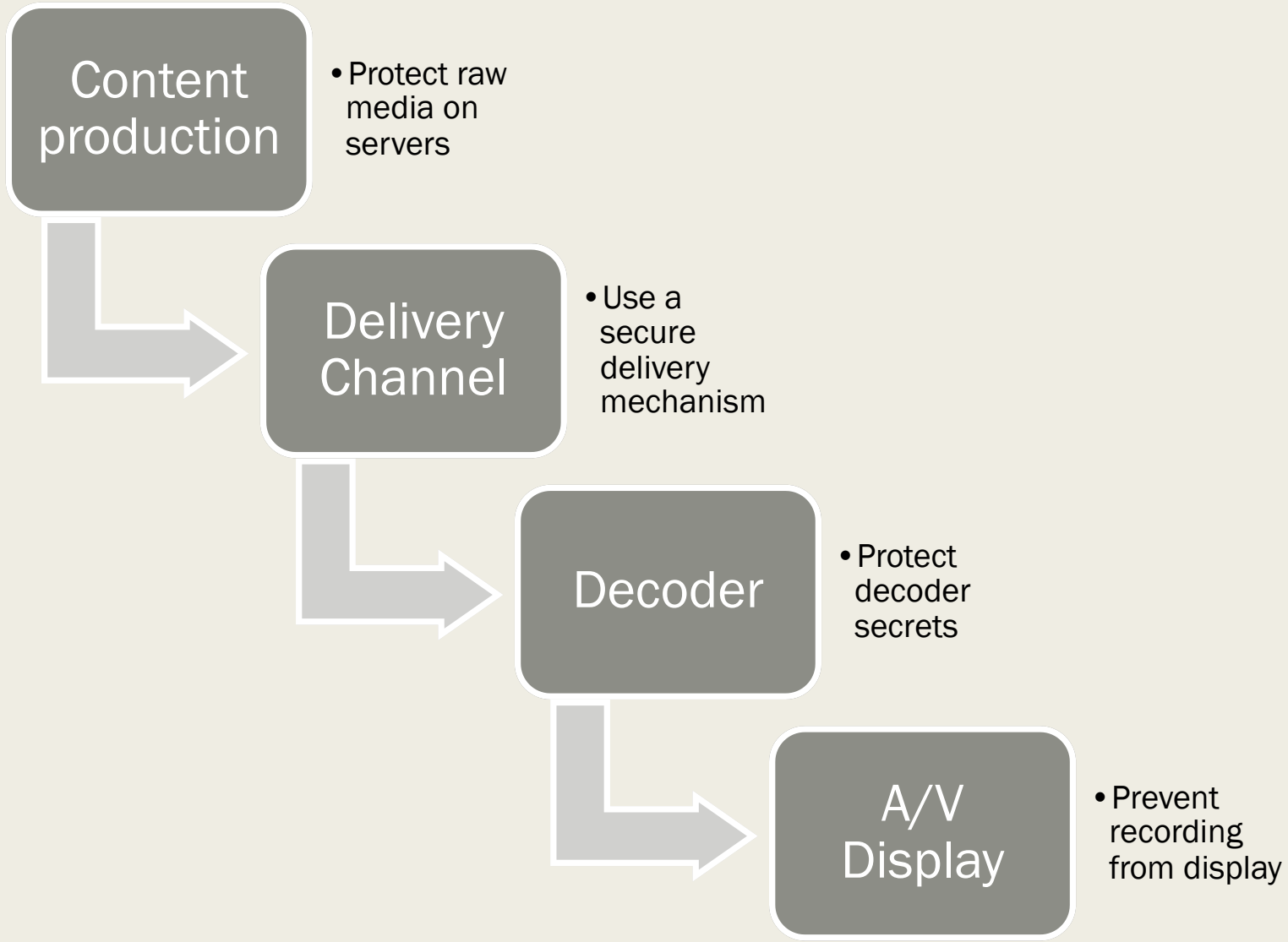
Circumnavigating

- Good OpSec
- TOR, VPNs or other proxy services.
  - *Route traffic through a non-blocking ISP*
- Transmitting disguised packets

- Obscure and deep links:
  - *Accessing the data through obscure domains or IPs*
  - *Onion sites*

SOURCE-TO-SINK PROTECTION

Trusted chains


Content production
• Protect raw media on servers
Delivery Channel
• Use a secure delivery mechanism
Decoder
• Protect decoder secrets
A/V Display
• Prevent recording from display

It’s about making it so hard it’s not worth it.

ONLINE VERIFICATION

	One time	Boot up check	Periodic Check
License check	One time check, usually during installation	Calls the server on bootup, but can be offline after	Periodically contacts license server to verify protection and license.
Data retrieval	Download game files from server	Key files are not copied to system on initial install and must be re-downloaded each time	Certain logic of the game is not included in the game and must be processed by the server.

Define “online”

- Intercept and fake the “verified by server” responses
- Fake requirements for offline-mode
- Patch out the verification in the binary
- Re-implement missing functionality

ANTI REVERSE ENGINEERING

(for interactive media)

DEF CON 23 - Chris Domas - Repsych: Psychological Warfare in Reverse Engineering

DEFCONConference • 96K views • 4 years ago

Your precious 0-day? That meticulously crafted exploit? The perfect foothold? At some point, they'll be captur

DEF CON 26 - zerosum0x0 - Demystifying MS17 010 Reverse Engineering the ETERNAL Exploits

DEFCONConference • 5.2K views • 1 year ago

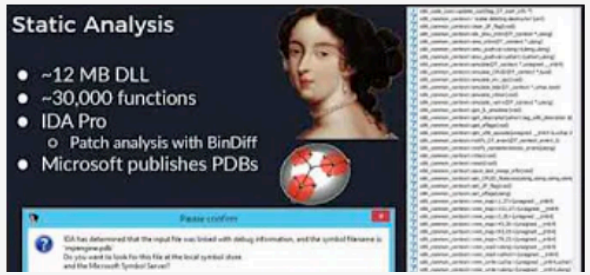
ating systems, fixing remote code execution

DEF CON 26 - George Tarnovsky - You Can Run but You Cant Hide Reverse Engineering Using X-Ray

DEFCONConference • 4.7K views • 1 year ago

Most of us have knowledge of PCB construction. In the past reversing someone's design was an easy

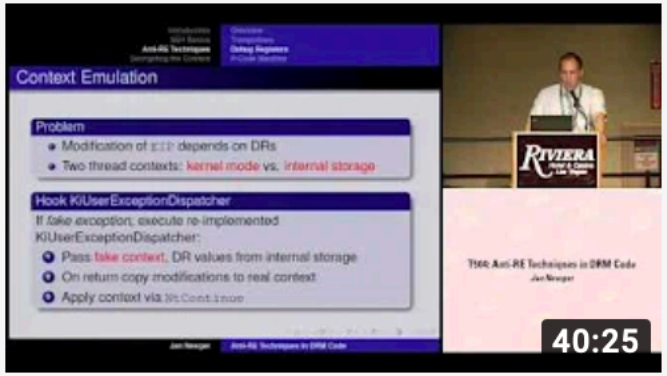
■ Use



DEF CON 26 - Alexei Bulazel - Reverse Engineering Windows Defenders Emulator

DEFCONConference • 28K views • 1 year ago

Windows Defender Antivirus's mpengine.dll implements the core of Defender's functionality in an enormous ~11 MB, 30000+ ...



DEF CON 16 - Jan Newger: Anti-RE Techniques in DRM Code

DEFCONConference • 138 views • 6 years ago

DEF CON 16 - Jan Newger: **Anti**-RE Techniques in DRM Code In order to **prevent** music from being copied among consumers, ...

AND NOW FOR SOMETHING MORE SPECIFIC...

CINAVIA

“Kills Camrips fast”

- Audio watermarking designed to withstand various distortion and signal cleaning
- Identifies a recording as a part of a given category:
  - *”Theatrical release”*
  - *”AACS protected home media”*
  - *“Preview release”*
- Playback device can be set to only allow certain types of watermarked media

The Watermark is a modulated audio data signal that is uniquely generated and adapted to each individual piece of content. Embedding is performed under the control of an advanced psychoacoustic model which continuously adapts the watermark embedding so that it remains below the threshold of audibility. This approach results in a Watermark that does not affect the audio quality of the content and is perceptually transparent to consumers in theatrical and home playback environments.

The Watermark Embedder does not process or modify the visual portion of the content.

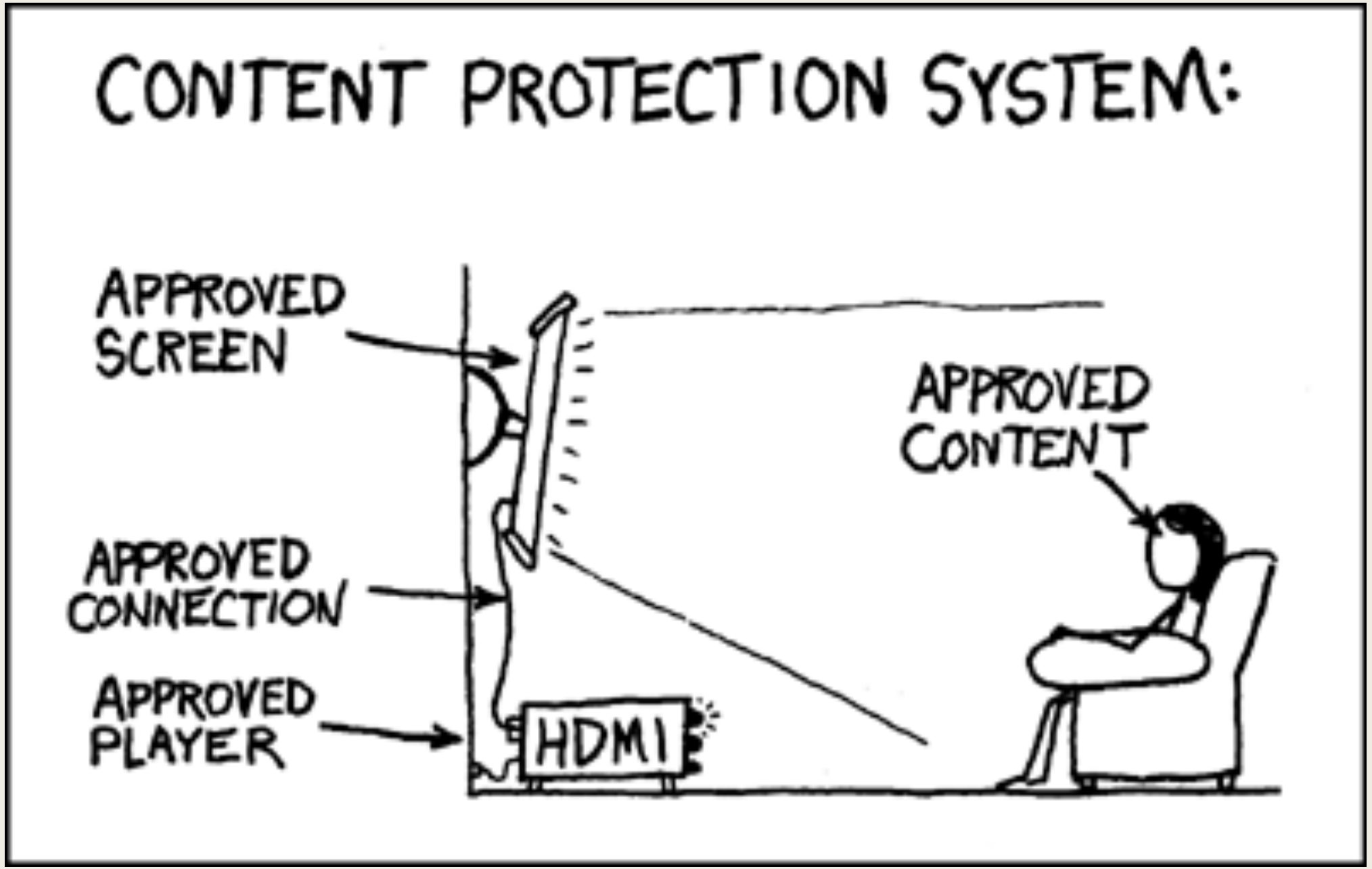
AUDIO CODECS	EFFECTS / ENHANCEMENTS	ANALOG ENVIRONMENTS
AAC / AACplus	Bass Management	Acoustic Propagation
ADPCM, to 2 bit/14 kbps	Compression / Limiting	Additive Noise, to 10 dB
ATRAC3	Echo / Reverb	Bandlimiting, to 1 kHz
Dolby Digital (AC-3)	Equalization	D/A-A/D Conversion
DTS	Error Concealment	Nonlinear Distortion
MLP	Multi-channel Down-mixing	Preemphasis / Deemphasis
MP2, to 8 kbps	Noise Gate	Speed Change, to +/-30%
MP3 / MP3plus, to 8 kbps	Pitch Shift, to +/-30%	Wow & Flutter
Resampling, to 4 kHz	Surround Encoding / Decoding	
Quantization, to 8 bit	Time Scale, to +/-30%	
WMA / WMAPro, to 5 kbps	Voice-Over	

Table 2. Examples of audio processing that Cinavia survives.

HDCP

High-bandwidth **D**igital **C**ontent **P**rotection

(aka/ the reason you're having trouble splitting that HDMI stream)



XKCD: Content Protection (https://xkcd.com/129/)

Cabling and Components: The Final Supply Chain

- Aims to prevent unauthorized media stream recording devices
  - *So you can't rip a film by playing it into a recording box*
- Devices identify themselves to each other to confirm authorization
- Also prevents eavesdropping on the cabling between two trusted devices
  - *All media traffic is encrypted between the devices*

A few tidbits from the spec

- Locality Check – The HDCP Transmitter enforces locality on the content by requiring that the Round Trip Time (RTT) between a pair of messages is not more than 20 ms.

All HDCP Devices contain a 128-bit secret Global Constant denoted by lc_{128}. All HDCP Devices share the same Global Constant. lc_{128} is provided only to HDCP adopters.

The HDCP Receiver is issued 1024-bit RSA public and private keys. The public key is stored in a Public Key Certificate issued by DCP LLC, denoted by $cert_{rx}$. Table 2.1 gives the fields contained in the certificate. All values are stored in big-endian format.

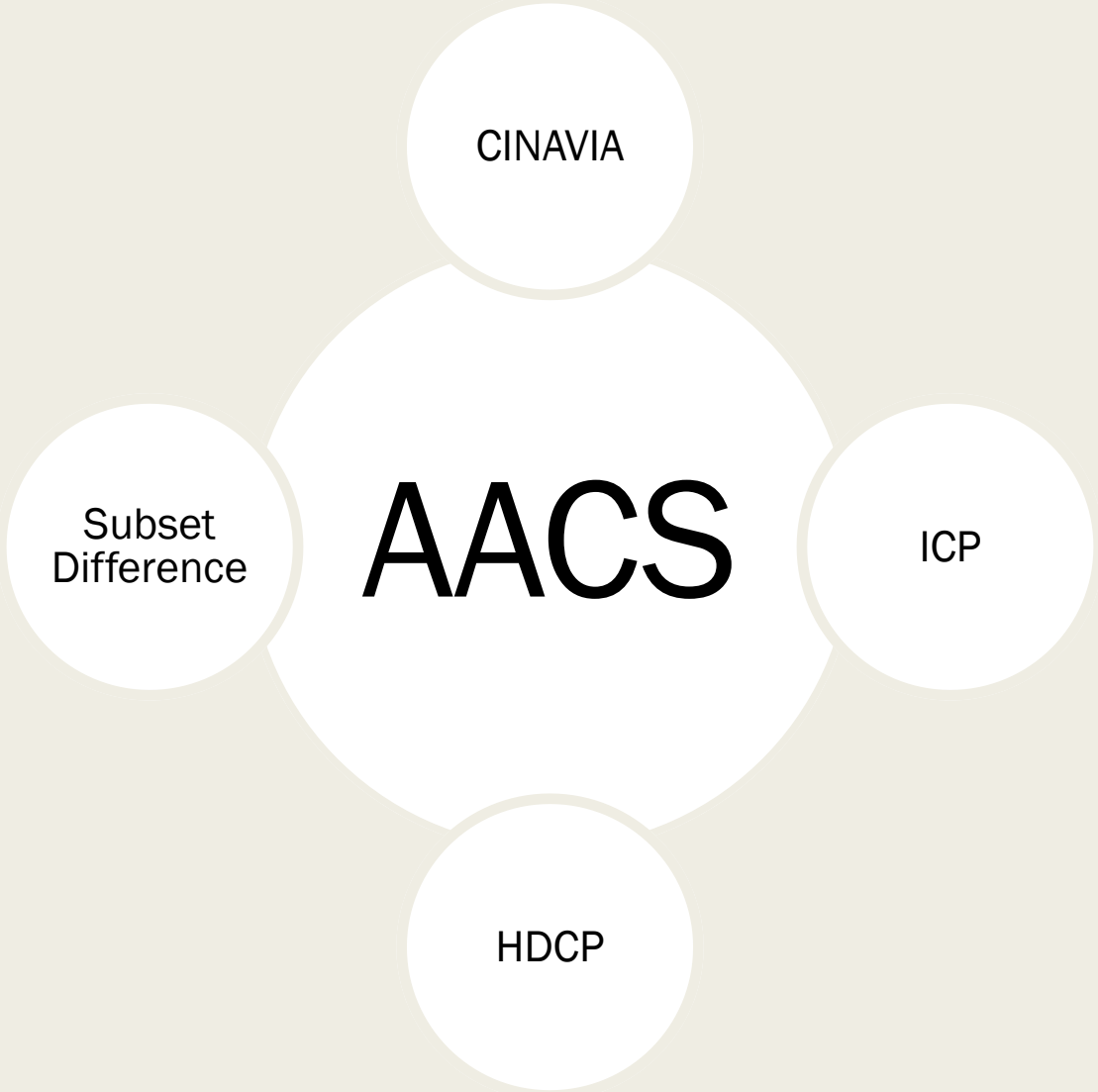
If you want more, search up “HDCP spec” and read it yourself

AACS

The Elephant in the room

First there was Content Security System (CSS)

- Used for DVDs
- Almost entirely broken:
  - *Basic media key encryption system.*
  - *DVDdecryptor is freely available online ~~and I've only had one DVD not work with it~~*


CINAVIA
Subset Difference
AACS
ICP
HDCP

ICP – Limiting quality on untrusted systems

- An Intel™ inclusion to the standard
- Allows media to specify that, if the HDCP chain is not available all the way to the sink, then quality should be reduced (ie/ 720p rather than 1080p)

Subset Difference: How does revocation work?

- Revocation only applies to any media created *after* the revocation
- All new media is encrypted using keys that are accessible by all licensed systems, except those on the revocation list.

Source to sink protection

- Drive must authenticate the PC system before providing additional data
  - *Protection from drive to decoder*
- HDCP checks may also be made.
  - *Protection from decoder to screen*

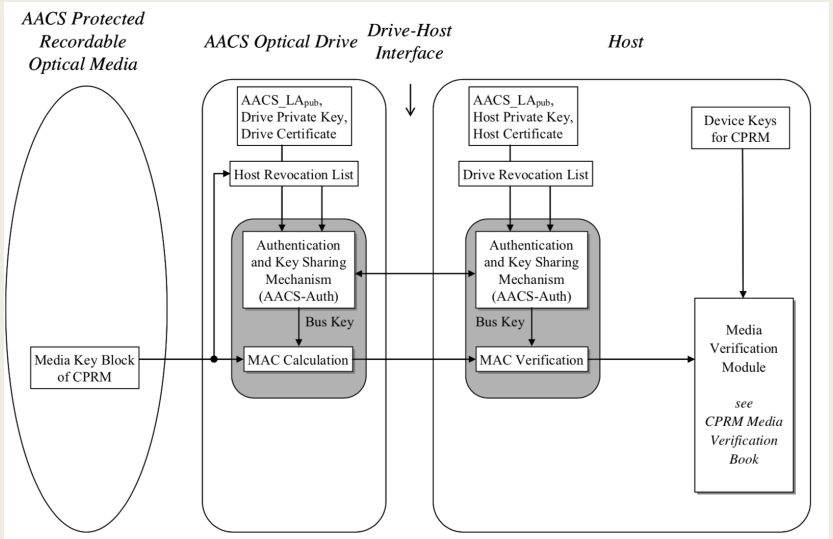


Figure 4-8 – Reading of Media Key Block of CPRM in a PC-based System

From AACS_Spec_Common_Final_0953.pdf, available from AACS LA

State of piracy

- We’re currently on AACS-71*
  - *There’s been 71 versions of revocation sets of device keys*
- BD ripping tools still work with the latest releases

*As of July 2019

The Tooling: AnyDVD, MakeMKV

- (This data may be out of date)
- Tooling often has 2 pricing tiers for purchase
  - *Online decryption*
  - *Offline decryption*
- In online mode, the disc's details are sent off to a remote server and a decryption key is returned
  - *Helps the tool creators to prevent discovery of their traitor keys*

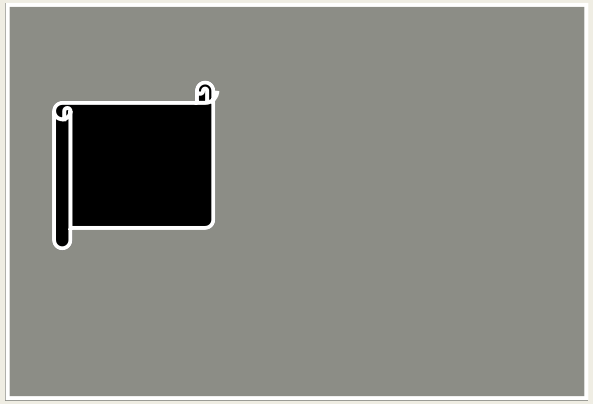
ONLINE DRM

Widevine, PlayReady, FairPlay et al

Widevine

L1	L2	L3
• Decryption, decoding and media control are performed inside a Trusted Execution Environment (TEE) • TEE should contain widevine keybox from the factory.	• Decryption is performed in TEE. Decoding and media control are handled by CPU (or otherwise)	• All functions performed outside TEE.
Mobiles and TVs	?	Browsers

Content Processing Server



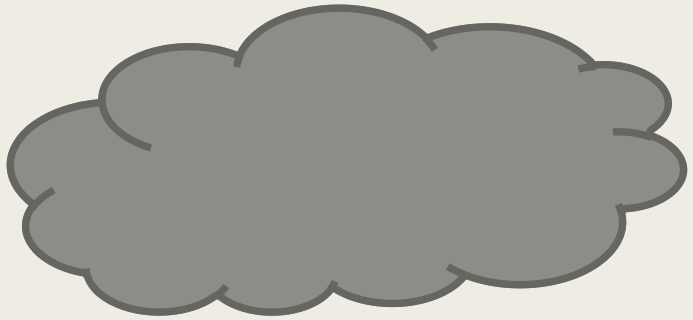
Hey License Server,
I have a file video called “Hackers(1995)” that I’d like to secure

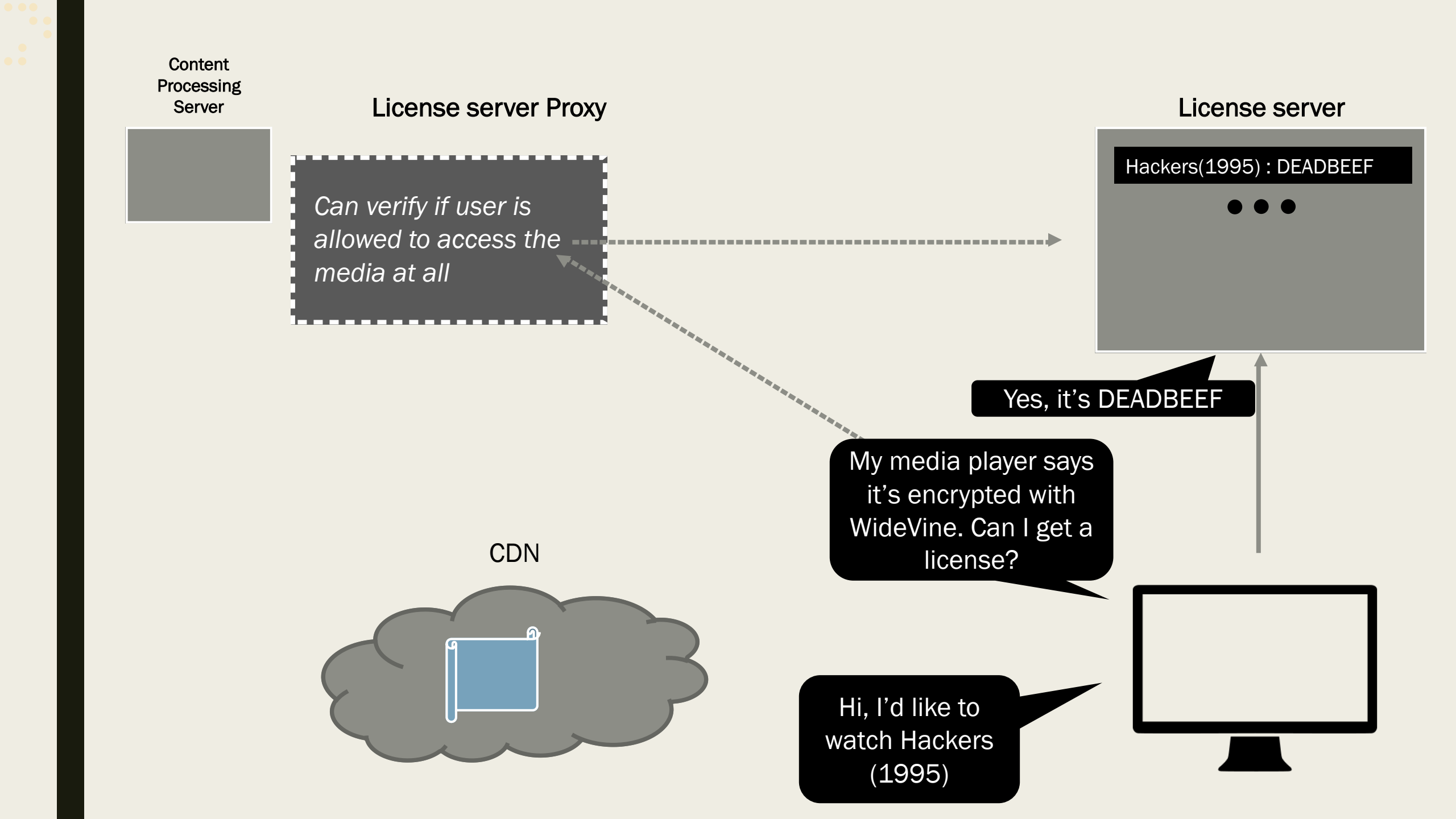
Okay, I’ve assigned it the key “DEADBEEF”

License server

Hackers(1995) : DEADBEEF

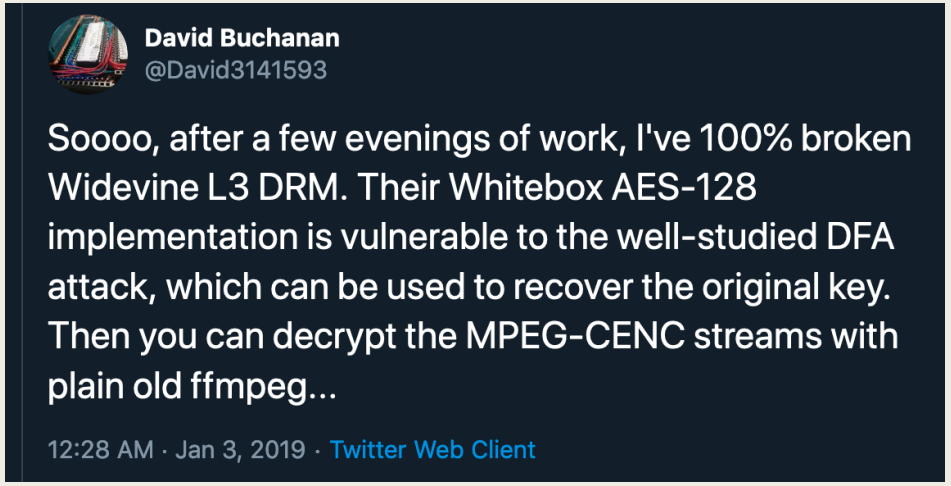
CDN




Content Processing Server
License server Proxy
Can verify if user is allowed to access the media at all
License server
Hackers(1995) : DEADBEEF
Yes, it's DEADBEEF
My media player says it's encrypted with WideVine. Can I get a license?
CDN
Hi, I'd like to watch Hackers (1995)

Has it been broken?

- L3:
  - https://twitter.com/David3141593/status/1080606827384131590



- L1: ???
  - *Requires the extraction of a keybox from the TEE*
  - *Breaking of Qualcomm's Secure Execution Environment (QSEE) might be used to expose some keys*
    - https://research.checkpoint.com/2019/the-road-to-qualcomm-trustzone-apps-fuzzing/

VMPROTECT

Runs Games in a non-standard VM

- Harder for crackers to read the instructions and determine what's going on.
- Slight performance penalty due to VM and emulations.

MISCELLANEOUS

These are just pretty neato

Nintendo splash screen: The side channel

- Designed for Nintendo's Gameboy range
- The cartridge must print the Nintendo logo to screen in the first seconds of boot-up
- The console verifies that the game attempts to display the logo and that it is the same as is present in its ROM
- Trademark infringement law is well understood and is much easier to get a cease-and-desist notice with.
  - *Copyright law can be unpredictable, especially across international boundaries*

The PS1 Wobble track: Just outside the specification

- PS1 games were written onto CD compatible discs
  - *So why can't I do a bit-by-bit clone of the disc?*
- The initial trial in of the track contains a set amount of track wobble
  - *No CD track is perfectly circular anyways, this is within spec*
- The PS1 disc reader has been built to find and decode this initial wobble as an encoded identifier
- No standard PC drive will even notify the system of such wobble
  - *Nor can you write the wobble*

Spyro the troll
(Spyro: Year of the dragon)

- Multiple levels of DRM
  - *Different levels of complexity*
  - *Different levels in enforcement*
  - *“Let them think they won early on”*
  - *https://youtu.be/4GYSeXLr5sY*
    - Also includes a brief explanation of the PS1 wobble

THE FUTURE OF DRM (?)

It will always get broken eventually

- Protect initial sales
- Fast identification of compromised sources and secrets
- Efficient revocation of access

Interactive media will push computations to the cloud (no offline modes)

Who was I?

My name is Rael

My Javascript skills pay the bills

My criminal record is clean

	E314c.github.io
	@E314cRael

ETC

QUESTIONS ?

References and Extra reading

- Making a Subset Difference: The crypto behind AACS
  - *Presented at BSides MCR '19, Recording on youtube. Slides on my github.*
- EFF's guide to printer microcodes
  - *https://web.archive.org/web/20180305181029/https://w2.eff.org/Privacy/printers/docucolor/*
- Earliest case of piracy:
  - *"Pirates of the Digital Millennium: How the Intellectual Property Wars Damage Our Personal Freedoms, Our Jobs, and the World Economy" by Jack B. Rochester; John Gantz FT Press 2004*
- Spyro DRM : https://www.youtube.com/watch?v=4GYSeXLr5sY

References and Extra reading

- PS1 Wobble: https://youtu.be/XUwS0fQ1D3c
  - *A more detailed explanation of the PS1 wobble and DRM systems*
- AACS Documentation:
  - *https://aacsla.com/aacs-specifications/*
- OverlordGaming - Youtube
  - *"Game piracy explained" - https://www.youtube.com/watch?v=8uUJFvSkTfI*
  - *"Film piracy explained" - https://www.youtube.com/watch?v=_wQcQgEMYuI*
- Qualcomm's Secure Execution Environment (QSEE) flaws
  - *https://research.checkpoint.com/2019/the-road-to-qualcomm-trustzone-apps-fuzzing/*
- "Mov is turing complete":
  - *https://www.youtube.com/watch?v=HlUe0TUHOIc*

REMEMBER:

A LOCK KEEPS AN HONEST MAN HONEST