

Jailbreaking and associated issues

- Lukas Zbranek
- Ondrej Antos
- Zdenek Riha

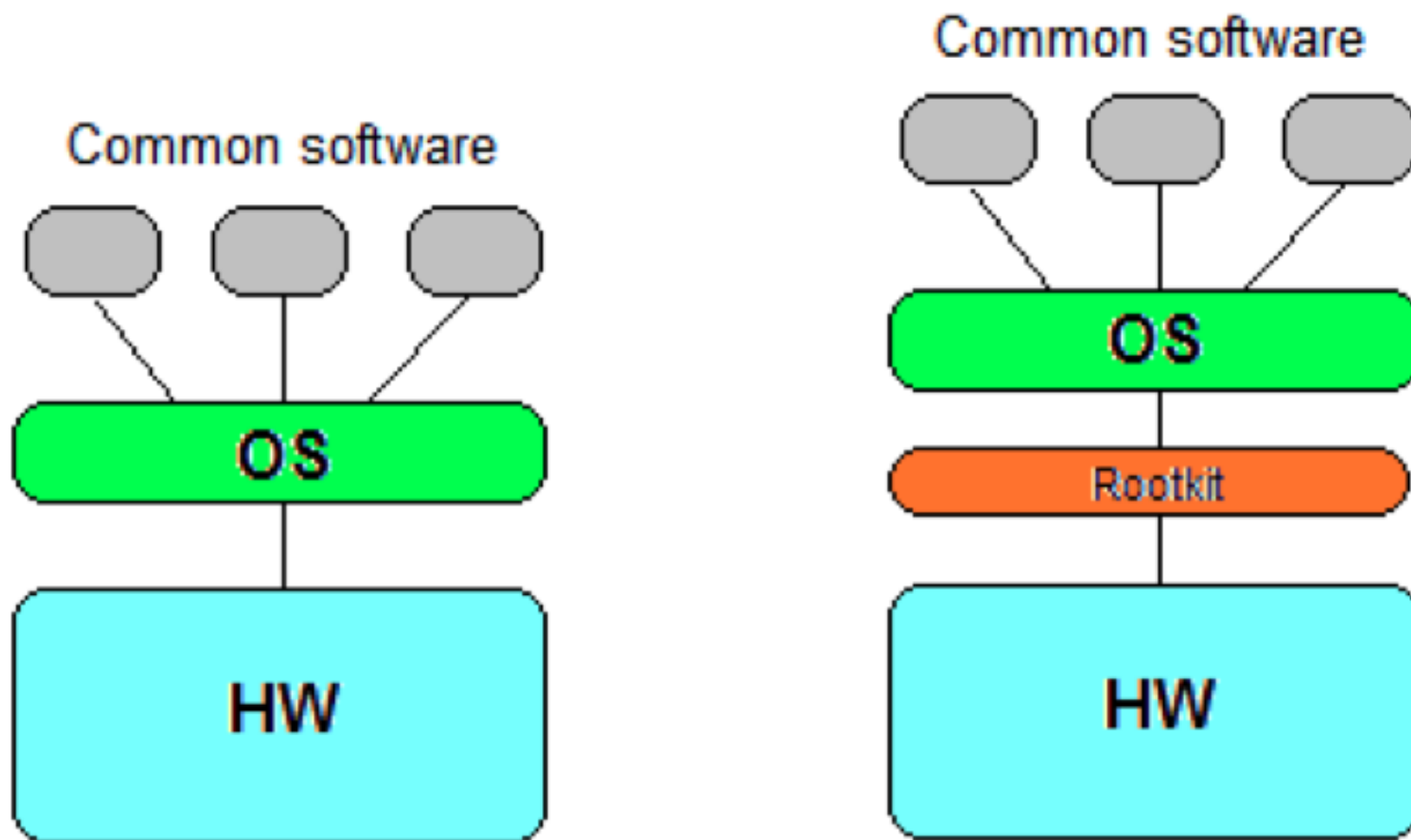
Protection circumventing in good faith

by Lukas Zbranek

Protection circumventing in good faith

- Investigation of technological protection measures (TPM)
- Prof. Alex Halderman proposed division of works into 2 classes:
 - TPM protecting literary works, sound recordings and audiovisual works – based on proceeding with Sony BMG and XCP rootkit
 - TPM protecting video games on PC
- First class was rejected because of existing regulation

Rootkit



Two Main TPM's

- Macrovision's SafeDisc – documented flaw, which affected almost billion computers
- Sony's SecuRom – no proof of security threat, only suspicion

Reasons for investigation

- Constant seeking to protect security of owned computer
- Sole research whether the game eventually the TPM creates security threat

Opponents' view

- Prof. Halderman didn't provide enough documented evidence of threats in connection with video games
- Already existing collaboration with security experts, who routinely identify flaws and help with finding the remedies
- There is no need for new regularization addressing this issue, because of existing statutory exemption applying to the security research

Result of proposition

- National Telecommunications and Information Administration has stated several factors based on information given by proponent and opponents
- All of them are in favor of fair use exemption.
- Legitimate research may be chilled without exemption
- Current exemptions may not be sufficient warranty for researchers
- → Exception has been recommended by Register of Copyrights

Circumvention of

• **dongle protection**

- Dongles = piece of hw, which is attached to computer (Parallel or USB port) and authorizes access to protected software
- Needs for circumventing such protection (according to existing exemption):
 - Dongle fails and became obsolete – there is no reasonable way, how to obtain legitimate dongle replacement

Proposal of new exemption

- Proposed by J. V. Montoro, Jr.:
 - Dongle becomes obsolete – failed to prove that is need of circumvention, when dongle works
 - Dongle fails and there is no replacement – proved, same as existing exemption
 - Incompatibility between dongle and OS – failed to prove, that there is no other option than using incompatible OS
 - Incompatibility between dongle and HW – failed to prove, that LPT port is obsolete

Result of proposition

- Register recommends class designated in the same way, as it was designated in 2006: ***Computer programs protected by dongles that prevent access due to malfunction or damage and which are obsolete. A dongle shall be considered obsolete if it is no longer manufactured or if a replacement or repair is no longer reasonably available in the commercial marketplace.***

DVD CSS legal circumvention

by Zdenek Riha

DVD CSS

- DVD
 - Digital Versatile Disc
 - DVD - Video
- CSS
 - Content Scramble System (a kind of DRM system)
 - Encrypts data (namely video) on the disc
 - CCS keys: authentication key, disc keys player keys, title keys, secured key disc set, etc.
 - Disc - specific keys stored in the lead-in area of the disc
- Long term keys are stored in DVD players
- Long term keys belong to DVD Copy Control Association

DVD CSS - Broken

- The aim of CSS is to
 - prevent copying disc (keys stored in lead-in) and
 - prevent playing content in non-compliant DVD-players.
- In 1999 CSS was broken
 - DeCCS by Jon Lech Johansen
 - Algorithm reverse engineered, keys brute forced
- CCS was replaced by newer algorithms in HD-DVD and Blue-Ray

DVD CSS - Reality

Nidesoft DVD Decrypter V5.1.06(Unregistered)

File Tools Edit Purchase Help

Open DVD Load IFO Crop Effect Trim

Movie	Original Length	Trimmed Length
F:\VIDEO_TS		
Title_01_01	00:58:56	00:58:56
Title_02_01	00:00:12	00:00:12
Title_02_02	00:00:32	00:00:32
Title_02_03	00:00:11	00:00:11
Title_02_04	00:01:06	00:01:06
Title_02_05	00:00:29	00:00:29
Title_03_01	00:11:14	00:11:14
Title_03_02	00:11:11	00:11:11
Title_03_03	00:01:15	00:01:15
Title_03_04	00:01:12	00:01:12
Title_03_05	00:00:54	00:00:54

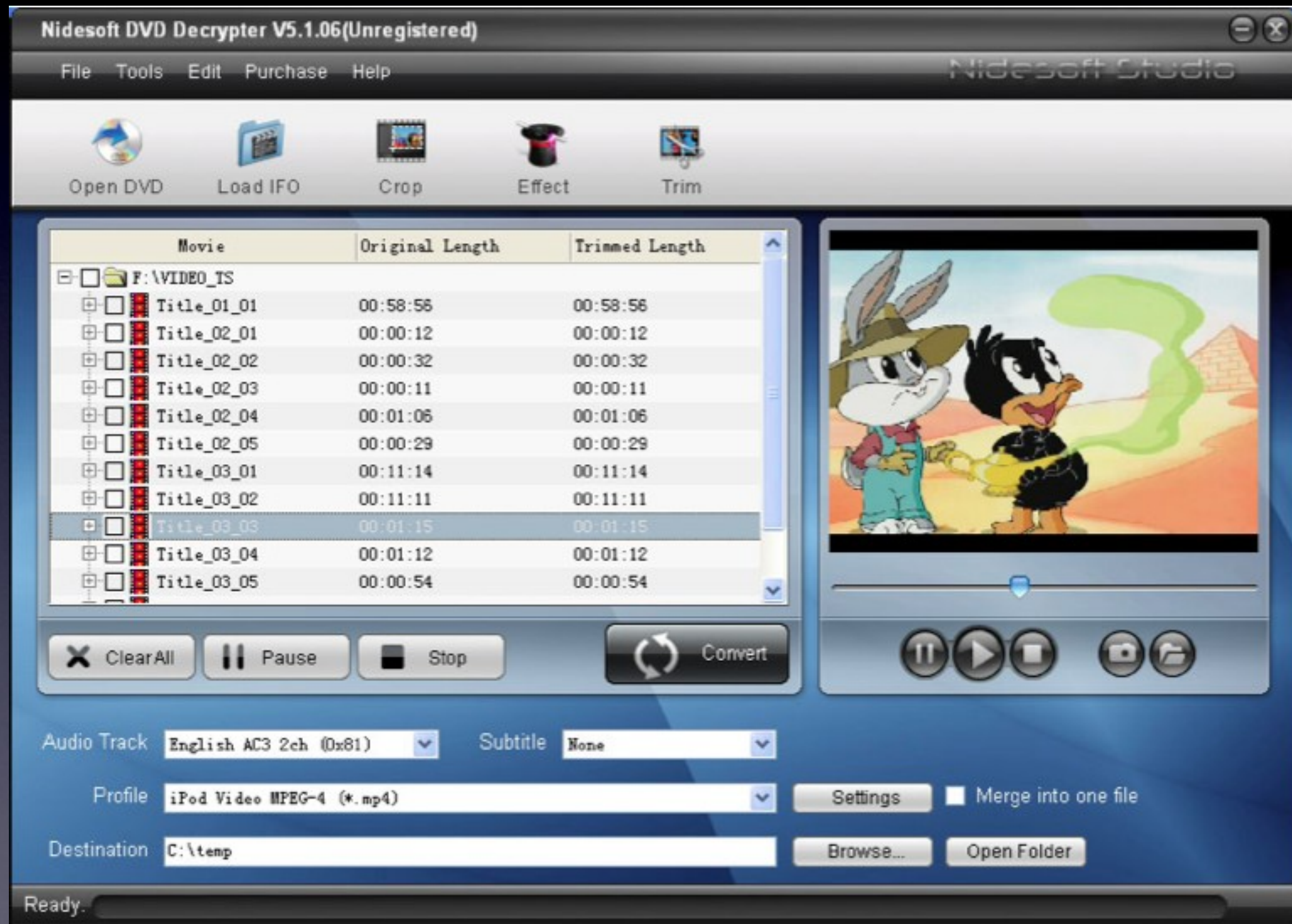
Clear All Pause Stop Convert

Audio Track: English AC3 2ch (0x81) Subtitle: None

Profile: iPod Video MPEG-4 (*.mp4) Settings Merge into one file

Destination: C:\temp Browse... Open Folder

Ready.



DVD CSS - Legal

Issues

- What can be done easily from a technical point of view does not have to be legal...
- DVD CSS circumvention legality depends on national legislation
- In the US the DMCA has been enacted in 1999
- Digital Millennium Copyright Act
 - Criminalizes circumvention of DRM (among others)
- Anti-circumvention exemptions possible
 - Reviewed every 3 years by Librarian of Congress

2010 DVD

Exemptions

- Motion pictures on DVD that are lawfully made and acquired and that are protected by the Content Scrambling System when circumvention is accomplished solely in order to accomplish the incorporation of short portions of motion pictures into new works for the purpose of criticism or comment, and where the person engaging in circumvention believes and has reasonable grounds for believing that circumvention is necessary to fulfill the purpose of the use in the following instances:
 - Educational uses by college and university professors and by college and university film and media studies students;
 - Documentary filmmaking;
 - Noncommercial videos. (A new exemption in 2010, similar to a previous educational exemption.)

Librarian of Congress

Exemptions

- Based on input (proposals) received from both the sides
 - E.g. educators and students
 - Representatives of copyright owners
- Educators and students claim that circumventing CSS is necessary as there are no alternative media not protected by DRM
- Representatives of copyright owners suggest alternatives to CSS circumvention

CSS Circumvention Alternatives

- Camcoding the movie with a videocamera from a TV screen
 - Not sufficient quality of image and sound
- Using video capture software
 - Does not capture all frames
 - Unwilling to provide a definitive answer whether this actually circumvents the protection ...
- Using VHS whenever available
 - Need for avoiding Macrovision's Analog Copy Protection (ACP)

Factors to take into account

- The availability for use of copyrighted works
 - Does the protection of the work enhance and/or inhibit the availability of the work for use?
 - Is the protected work available in other formats?
 - Are alternative means of accomplishing the noninfringing use available to users?
- The availability for use for nonprofit archival, preservation, and educational uses ...
- The impact that the prohibition on circumvention has on criticism, comment, news reporting, teaching, scholarship, or research.
- The effect of circumvention on the market for or value of copyrighted works.

Individual cases

by Ondrej Antos

Cloud - based video

- Video on demand service
- Restrictions considering hardware and software platforms
 - Netflix case
 - Online access
 - Does not have correct hardware and software

Cloud - based video

2

- Enough alternatives
- Mere inconvenience



DRM servers

- Sound recordings, audiovisual works and software
- DRM authentication entity is remotely operated
- If switched off, customers lose access to their purchases
- Google Video Express, Microsoft's MSN Music Store, Yahoo! Music

DRM servers 2

- Arguments:
 - Denial of ability to access lawfully purchased content
 - Circumvention is happening on already purchased content, therefore has no commercial impact
 - Librarian argument

Exemption for investigation

purposes

- Possibility to jailbreak DRM protection for use of protected content
- Provider would have to supply a content in question on demand without any DRM protection
- Forensic analysis has already a unique legal solution

Broadcast flag issue

- A digital “watermark” added to DTV signal which prevents audiovisual work to be recorded and then accessed at a time different to moment of broadcasting
- Not in use today
- Rejected as “highly speculative scenario”

Image Constraint

Token - ICT

- Embedded in physical medium
- Resolution is downgraded when connected to display through any “untrusted” analog connection
- HDMI (High Definition Multimedia Interface)
- HDCP (High - Bandwidth Digital Content Protection)



HDMI

Ebook controversy

- DRM embedded in ebooks denies access to it by read-aloud function or rendering into a specialized format
- Considering .PDF files with restrictions and Microsoft's .LIT files
- It denies blind and sight - impaired people to access content of books even though the technology itself is advanced enough

Thank you!