= BackupHDDVD =

BackupHDDVD is a small computer software utility program available in command line and GUI versions which aids in the decryption of commercial HD DVD discs protected by the Advanced Access Content System . It is used to back up discs , often to enable playback on hardware configurations without full support for HDCP . The program 's source code was posted online , but no licence information was given .

Written by an anonymous programmer using the handle Muslix64 , BackupHDDVD is distributed with none of the cryptographic keys necessary for decryption . Users wanting to use the software to decrypt a protected disc 's contents must obtain the appropriate keys separately , a task with which neither the original author nor his or her versions of BackupHDDVD assist .

BackupHDDVD represented the first known successful attack against AACS . The utility circumvents content protection by decrypting video files directly with AES , the underling cryptographic cipher used by AACS . Using this technique , BackupHDDVD is able to completely bypass the AACS chain of trust , rendering it immune to revocation . The cost of this immunity is that users are forced to rely on keys leaking from commercial player software to use BackupHDDVD with new discs .

= = History = =

According to the creator of BackupHDDVD , he or she first set out to circumvent AACS to bypass a restriction in software HD DVD players which reduced the quality of AACS restricted 1080p high definition video to that of standard definition DVD video or refused to play outright unless an HDCP compliant chain of video hardware was present . At the time only a few computer monitors and video cards supported HDCP . As a result , configurations that would have allowed high @-@ definition HD DVD viewing in software players were exceptionally rare .

On December 18 , 2006 , a video which showed BackupHDDVD being used to decrypt and copy the film Full Metal Jacket to a hard drive was uploaded to YouTube . Two days after the video was uploaded , the initial version of the utility along with its source code and documentation was uploaded to a file hosting service . A link to the file was then posted by the utility 's creator on the forums of Doom9 , a website devoted to DVD backup . The utility 's documentation , along with the forum post , contained little information as to how necessary keys could be obtained . The author elaborated in another forum post , claiming that keys could be obtained by exploiting the necessity for them to be held in memory to allow playback in player software .

On January 2 , 2007 , the author posted the 1 @.@ 0 version of the BackupHDDVD utility , which included support for the decoding of discs using volume keys . For several weeks following the utility 's release no success using the author 's key extraction technique was reported . In mid @-@ January 2007 , a volume key was published by another member of the Doom9 forum along with an explanation of the technique used to obtain it . Other forum members quickly discovered keys for different titles . Keys for many discs are now readily available on the internet .

Further development of BackupHDDVD was being hosted on SourceForge until the site received a DMCA takedown notice alleging a violation in late February . In compliance with the notice , the project was immediately removed . Several versions of BackupHDDVD have been released by individuals other than the original author , including some versions with GUIs and the ability to locate keys on the internet or scan for them in memory automatically . HDDecrypter , a port of BackupHDDVD to C with a native Windows GUI is also available . This version supports multiple CPU threads and runs faster than its Java counterparts . While development of BackupHDDVD has ceased , a commercial HD DVD decryption utility called Slysoft AnyDVD HD exists which relies on compromised AACS processing or media keys to allow for the backup or unrestricted viewing of any AACS @-@ protected discs without the need for title or volume keys .

= = Background = =

The AACS Licensing Authority (LA) assigns a series of 253 unique cryptographic keys to device manufacturers . When an AACS protected disc is manufactured , a series of up to 64 keys called title keys are generated and the video content on the disc is encrypted using these keys . The title keys are stored on the disc and themselves encrypted with another key called the volume unique key . The volume unique key for any disc can be calculated by all authorized devices using another key called a processing key , which is derived from a media key block stored on each disc . Authorized devices use one or more of the manufacturer 's assigned device keys to decrypt the media key block , yielding a processing key and enabling further decryption of the volume and title keys , and finally the content .

If a device key is to be revoked , the media key blocks on all discs manufactured after the time of revocation are encrypted in a way which does not enable the revoked device to obtain a valid processing key . Users trying to view new content on a revoked player would be forced to upgrade their player software to a more secure version , thereby limiting the scope of the compromise each time an exploit is discovered . While a compromised device or processing key could be used to decrypt a large number of discs , BackupHDDVD does not use these keys because they can be revoked by AACS LA . Because the AACS revocation system works by preventing a given device or player from calculating a valid volume unique key , BackupHDDVD circumvents the system entirely by relying on volume or title keys leaked from authorized players . With these keys BackupHDDVD is not subject to device revocation and is able to decrypt the content directly , bypassing the key exchange and verification process .

= = Features and limitations = =

Users must have either found decryption keys themselves or obtained them elsewhere for most versions of BackupHDDVD to work . The utility reads a text file containing volume or title keys and attempts to find a set of corresponding keys for the inserted disc . Through a standard AES library , it then decrypts each video file on the disc using the appropriate keys and writes the results to a location specified by the user . Direct file decryption allows the utility 's functionality to remain unaffected by device key revocation and its performance unencumbered with AACS overhead .

Originally intended to be a proof of concept , BackupHDDVD is severely limited in its ability to produce fully functional copies of commercial discs . Early versions were unable to properly decrypt discs which used the in @-@ movie experience technology . New versions work around this limitation by excluding interactive content from decrypted copies . The utility cannot process HD DVD navigation functionality which enables menus , chapters , secondary audio tracks and subtitles , so these features are inaccessible in copies created by BackupHDDVD . Most versions provide no validation for keys and will still attempt to decrypt a disc 's contents with an incorrect key , resulting in corrupt files .

= = Legality = =

Under United States anti @-@ circumvention law created by the Digital Millennium Copyright Act , BackupHDDVD may qualify as a device primarily intended to " circumvent a technological measure that effectively controls access to a [protected] work . " If identified as such , it would be illegal to use or distribute .

= = Reaction = =

Reaction to the utility by Doom9 forum members , bloggers , and mainstream media has ranged from supportive to intensely hostile . By some , the circumvention of AACS was seen as a reaffirmation of fair use . Others felt that the utility was no more than a piracy tool and would bring about group punishment against consumers in the form of player revocation . One article compared proponents of BackupHDDVD to terrorists . When the release of the tool was first publicized , several articles claimed that AACS had been cracked . In fact no cryptographic weaknesses

constituting a crack have yet been found in AES , the underlying cryptographic system of AACS . Keys are actually obtained through a side @-@ channel attack .

Initially , it was thought that the compromise of HD DVD 's security would entice some studios into adopting the competing Blu @-@ ray format , but Blu @-@ ray 's AACS implementation has since been circumvented using a similar method . However , Blu @-@ ray offers an additional layer of protection called BD + .

There was some speculation that the player used by the utility 's author to obtain keys would be revoked . Cyberlink , which sells the PowerDVD player software , was quick to deny that its software could be used to obtain keys . Corel was silent about the role its WinDVD software had played in the leaking of volume and title keys . Both companies have since released updates for their player software .

The consortium behind the HD DVD format and the studios delivering films on the format did not release an official statement beyond that they were investigating the utility . On January 24 , 2007 AACS LA issued a statement acknowledging that AACS security had been compromised while urging software vendors to limit the availability of keys in memory . Beginning with discs manufactured in late April , versions of PowerDVD and WinDVD responsible for leaking keys have been revoked and free updates are available to owners of affected versions .