HDCP - Barriers or security?

Have you ever 'beat' your DVD movie disc yourself? People often want to save a DVD movie on their hard drive or burn another DVD to prevent a damaged or lost original disc, or for some reason. But only a few people actually do this, yet

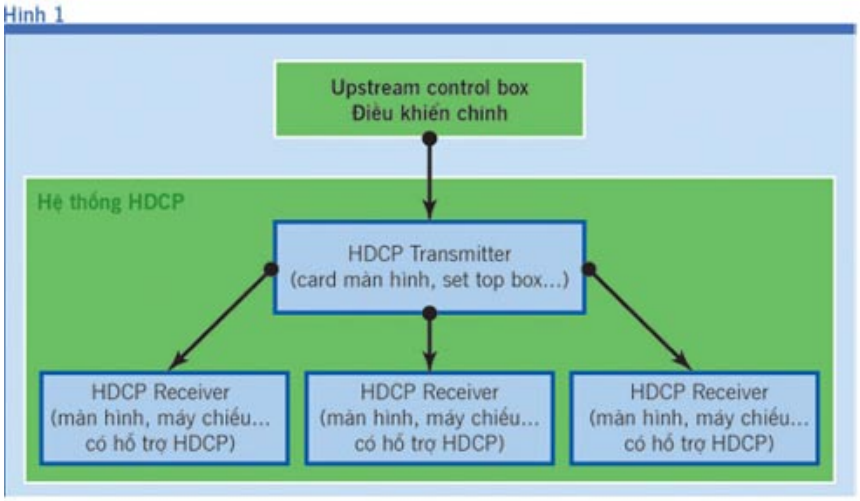
Have you ever "beat" your DVD movie disc yourself? People often want to save a DVD movie on their hard drive or burn another DVD to prevent a damaged or lost original disc, or for some reason. But only a few people actually do this, not to mention whether it is legal or not. In the DVD world, we can copy DVDs because of a young man named Jon Lech Johansen (nicknamed DVD-Jon). It was Jon who broke the DVD protection barrier so that ordinary users could copy DVDs freely on the hard drive. And actually, without Jon's "hand" embedded, Linux users won't be able to watch DVDs on this operating system.

In the last few years, we "live" quite comfortably in this DVD world because we can easily do everything when we have a DVD movie. This is the problem of studios around the world, but "pain" is still Hollywood. Therefore, Hollywood is looking for ways to increase security, not allowing users to decode and copy movies to the hard drive. The next step, Hollywood will partner with Intel, Macrovision and Digital Content Protection LLC to come up with new and hopeful methods that will soon emerge.

One of the most recently mentioned anti-piracy methods is HDCP (*High Bandwidth Digital Content Protection*). This method not only prevents copying from the original disk to the hard drive, but also further, blocking even those that are copied illegally from being displayed on the screen.

Copy protection is no longer just software, but also hardware. Specifically, HDCP not only needs support from the operating system, but also requires hardware devices to support, you can watch an HDCP protected movie. No matter if you are an original HDCP owner, there is no HDCP-compatible device, so you can't watch it.

So, what exactly is HDCP and how does it "run"? What will devices like watching movies in future paychecks look like?



HDCP definition

Original, HDCP is molded by Intel's hand, in the form of a protocol for protecting high-definition (HD) content transmitted via DVI (*Digital Visual Interface*) and HDMI (*High Definition Multimedia Interface*). The first technical version of this protocol appeared long ago, in September 1999. So far, it has been version 1.2a on May 10, 2006.

HDCP's goal is to prevent users from viewing or copying HD content on unauthorized devices. We can attribute HD content in 3 forms:

1. Movie on HD DVD and Blu-ray disc.

2. High-definition TVs are broadcast through set-top boxes, via cable or broadcast mode.

3. High-resolution source via computer graphics card (games, movies or other video content from the computer to the screen).

The common security method of HDCP is to use key exchange architecture (key-exchange). One of the main features of HDCP is the ability to "recover" the key that the manufacturer (studio and device manufacturer) sets.

For example, if a user tries to project an HD DVD or Blu-ray movie on their computer using an unlocking software (such as DVD Decrypter, AnyDVD .), the computer will record and notify This is done with a central key (authority) mechanism, retrieving and "cataloging" this "fake" key into "blacklist". At that time, users will not be able to use that computer (configure the machine). The feature will be saved) to watch HD movies too.

If you use certain software to bypass HDCP then the screen will turn white, or a "lovely" dialog will show that you are trying to do something "illegal". Currently, hardware protection in collaboration with such software is supported by many device manufacturers.

However, it is not surprising that many hardware equipment manufacturers in the computer world are quite shy when "touching" HDCP. You can go to this address to see a list of companies that accept copyright protection agreements and will apply the HDCP protocol in their hardware products: http://www.digital-cp.com/list . This list is quite long (about 400 companies). The two companies "most passionate" with HDCP are Warner Brothers and Walt Disney studios. Movies from these two studios (HD DVD or Blu-ray) will be protected if viewed via

HDMI or DVI. What about other studios? They have not yet jumped on the HDCP, perhaps waiting for public opinion before deciding whether or not to bring HDCP to their movie disc.

Inside HDCP

It can be said that HDCP's internal workflow is similar to the principle of a protocol in the sense that protocol is a method that a specific system uses to communicate between components. To understand it, we must have a clear view of the objects in the environment of HDCP. In Figure 1, we see 3 basic components: Upstream control (U), HDCP Transmitter (T) and HDCP Receiver (R). Only when there are 3 basic components is there a real HDCP environment.

In this environment, between HDCP Transmitter and HDCP Receiver there is an identification mechanism before the devices can work together. This identification will occur when T sends a communication signal to R. If the device displays compatibility, it will return the command to T using the device lock set issued by Digital Content Protection LLC.

Next, T will compare this key set with its own device key. At that time, the system will conduct the check (table checksum) compatibility between 2 devices via dynamic memory and complete the identification.

The above mentioned sounds very good, smooth and simple. But how can they run the same beat?

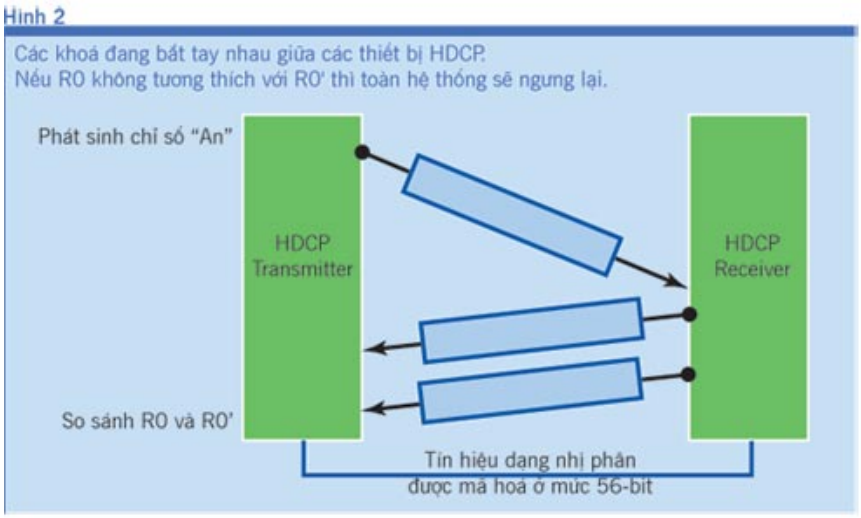
HDCP works

Any device that wants HDCP compatibility must have 40 secret 56-bit encrypted key files. These keys are collectively called: Device Private Keys. The easiest way to visualize these keys is that they are like fingerprints. No device has the same coding set, at least in theory. Digital Content Protection also puts a "header" into each of the 1 header key files called KSV (Key Selection Vector). This is a 40-bit binary value. The process of exchanging devices with these interactive keys is illustrated in Figure 2.

First, to communicate between devices, T sends a "hello" message containing a KSV of T itself (Aksv) to R. If this first contact is "ok", the function controls this calculation. "hdcpBlkCipher" will give "An" a value. Then, R sends back its KSV (Bksv) to T. At that time, if the identification is questionable, T will check again (possibly checking the user's home phone number) to make sure HDCP Receiver keys are not revoked previously (or if they are falsified, the system will disable the device key). If you pass the identification process, can you "open the fence" for digital content to go through? This time is not completely clear. The system will have to check the mentioned checksum table above. According to HDCP specifications, the checksum table is a 56-bit binary based on the "An" value of 2 KSVs. If the value of R0 does not match R0 ', the identification process will be repeated (Figure 2).

This is even more complicated if the environment has different HDMI / DVI connections, and HDCP Transmitter and HDCP Receiver must perform multiple detection. On the other hand, there is a third class of identifiers added to each process. Each "frame" of data transmitted over an HDMI / DVI cable will be detected again every 2 seconds.

Finally, the system ensures that the content is protected not only in the movie disc layer but also in the display layer. Because security is built right into the hardware device, the barrier is very difficult.



What about users?

Despite the hype, companies that want to soon bring HDCP into their products are not yet popular. ATI and NVIDIA said their graphics cards are compatible with HDCP, their products work well with upcoming high-definition content. This may be good news because the GPU is capable of exporting images at 1080i / p, but as we mentioned, HDCP is not the only factor in resolution. The problem is that HDCP keys from the central key-authority corresponding to the display device have not yet been "transplanted" on the graphics card. Furthermore, it is not possible to use the BIOS update method to include these keys in the graphics card because the empty addresses within the PROM are very limited and have priority for graphics scripts. The most feasible way is probably the graphics card needs a new chip designed specifically for this purpose; Graphics card currently not available.

Therefore, even the latest NVIDIA cards such as 7900GTX with LCD monitors support HDCP, you cannot see HDCP movies as advertised. The screens that really support HDCP are just beginning to appear. Most modern screens have "HDCP compatible" stamped but are based on the old HDCP standard (1.0, now 1.2a). This will cause many obstacles for those who want to be the first user of HDCP. You can learn more about this issue at http://www.firingsquad.com/hardware/ati_nvidia_hdcp_support. In the table below is a list of some of the screen models that actually support HDCP. If the monitor does not have HDCP support, the device and graphics card are incompatible, or do not support HDCP, then when using HD DVD or Blu-ray discs, integrate the lead-in security bit, user will encounter the following situation:

• A blank screen will appear, informing you that the device does not support.

• The video version shows only at 480i / p resolution.

Some companies, such as Sony, have abandoned the decision to set up an ICT flag in their video discs, due to excessive pressure from consumers and the need to encourage Blu-ray access to the living room.

HARDWARE INTERVENTION

Because HDCP is a security solution that combines software and hardware, it is much more difficult to disable it. Surprisingly, the market now has some hardware products through HDCP, that is "HDCP strippers".

Currently, German electronics company Spatz launches two products to bypass HDCP: DVI HDCP and DVI Magic. These two devices operate in a way that does not touch HDCP technology, instead, it uses the same HDCP chip as the HDCP-supported monitor. These devices "lie" between the source device and the display device, which is responsible for separating high-resolution video signals from HDCP.

Therefore, the HDCP signal source from the player will also be displayed completely in the box without this screen. Then, its next task is to convert the video into RGBHV format or a non-secure DVI signal. Therefore, monitors that do not support HDCP but support resolutions up to 1080p / i or PAL / PAL Progressive to NTSC / NTSC Progressive can display high definition video. It is possible that analog, digital, LCD or conventional CRT monitors do not support HDCP.

HDCP decoding: Spatz's DVIMAGIC HDCP device can overcome the HDCP barrier

Live with HDCP

Table: These are HDCP compatible screens adopted on May 10, 2006.

Brand **Model**GatewayFPD2185WHPF2105NECMultiSync 20WMGX2SamsungSyncMaster 244TViewSonicVP2330WBDell3007FPWDell2407FPWDell 2007HDWSamsung214TSamsung930MPSamsung940MWSamsung242MPSonyMFM-HT95SonyMFM-HT75W

HDCP has appeared in the entertainment and home electronics entertainment market and is widely accepted. What about the computer market? The future of HDCP in this market is not simple. There are many sources who believe that the HDCP protocol itself has been "cracked". In 2001, documents indicating the weaknesses of this protocol were "exposed" to the public. Some of the first cryptanalysts who discovered the defect of this protocol are Scott Crosby (Carnegie Mellon University) and Ian Goldberg (Zero Knowledge Systems). According to Crosby, he can fully control the central key-authority mechanism, and he points out that if enough keys are available, one can get the correct checksum between the two devices, and then release the key. "fake" to make the device compatible with HDCP, or disable system validation.

In addition to Crosby, another cryptographer, Niels Ferguson, has said that he has unlocked the HDCP mechanism, but did not publish his research because he was afraid of problems related to digital copyright law.

But there's another layer of security, HDCP + Certs. One hypothesis is the central key-authority mechanism that adds encryption certificates to key files. This means that each device will have a unique new "identity card" issued by the celtral key-authority, which can be created using standard algorithms, such as RSA / DSA. In this way, the HDCP Receiver will send a public key and include a "identity card" and will be identified by the other end both.

HDCP has initially revealed its flaws, a "wound" of Intel. Due to the linear key exchange mechanism, when data is transmitted from one point to the next, it is not possible to exclude the possibility that data will be "peered" or reduced. 56-bit chemistry, "contact" lock files between the Transmitter and Receiver are easily counterfeited.

You will agree that HDCP technology is strong or weak depending on which side you are standing on. If standing on the side of studios who want to manage products, want users to "go", then HDCP is weak. In the face of users who want to see the movie they bought at the highest resolution supported by the film, they have a lot of hope. In any case, HDCP is more "resilient" than security standards before it, so it will certainly not be so easy to be "broken".

Finally, whether you like it or not, the future is coming, HDCP will still "reign" on store shelves. If you want to buy the most fashionable products at this time, you should consider and be aware of HDCP compatible version 1.2a. If you want to watch HDCP on your computer, you have to wait for the HDCP card to support completely.

To know if the system is compatible well with each other, you can go to www.simplayhd.com to check.

HDTV AND AWARENESS USERS

Do you really have a high resolution TV?Or are you planning to buy one?How do you know if the image you are viewing on the correct TV is a high-resolution video?What are the concepts of DTV, HDTV, HDMI, DVI, HDCP?In essence, how is the new copyright mechanism?A series of questions can make us "shocked".

HDTV - High-Definition Television: the standard that the US will apply to all new TVs in the near future. Compared to the current system, HDTV has 2 important changes - analog (analog) signal is converted to digital signal and image quality is raised. New generation TVs will gradually be "wearing" HDTV. However, the US Federal Communications Commission (Federal Communications Commission) issued a term from March 1, 2007, all new TVs must switch to a digital tuner to be able to receive shape transmissions. number; analog broadcast wave will no longer be played after April 7, 2009. Obviously this is the first standard of an HDTV agreed by every company.

The second part of HDTV is that the image quality is not yet clear. The easiest way to identify HDTV is to check the pixel density. The more pixels on a screen area, the higher the image quality. Specifically, if comparing 2 analog TVs that receive the same source, the smaller screen TV will give a better picture because it has the same number of pixels but the display area is smaller so the pixel density is thicker than the TV with the screen. large image. Another problem affecting image quality is the frequency and method of "refreshing" the screen. If stopped at resolution, the following parameters can be displayed on analog TV as well as the number:

• 300x360 pixels - VHS quality - standard VCR tape.
• 460x360 pixels - television - TV stations use.
• 560x360 pixels - VCD quality.
• 720x360 pixels - DVD quality.
• 640x480 pixels (480i or 480p) - DTV standard for both i and p.
• 1280x720 pixels (720i or 720p) - DTV standard for both i and p.
• 1920x1080 pixels (1080i or 1080p) - DTV standard for both i and p.

HDMI and DVI

If your TV is digital and is in the 1080i compatible list, that's good news. But this is still not eligible for HD viewing. To watch HDTV, you need to use one of two types of communication / cable: HDMI or DVI. DVI used to be a connection between a computer and a monitor and HDMI was the connection standard for home entertainment devices.

Currently, although many manufacturers of electronic devices labeled HD-Ready, HD-Capable, HD-Compatible

. on their newer TVs, few TVs have HDMI or DVI terminals. What's worse is that if the current TV sets are not compatible with HD, the manufacturer will not make clear, confusing buyers. Previously, at consumer electronics fairs, Microsoft and Sony were excited and flattering for their Xbox 360 and PlayStation 3 children. They promised to play games with HD quality much better. However, both Microsoft and Sony have just launched products to show HD movies. Microsoft has a bundled product for the Xbox 360 to watch HD DVD movies, while Sony's PlayStation 3 (PS3) will include a Blu-ray reader.

Sony plans to release two PS3 versions - high prices; Low price version does not have HDMI output. The Xbox 360 does not have any HDMI output on the current two versions. Neither the Xbox nor PlayStation has DVI. Therefore, according to HDCP security standards, neither the Xbox 360 nor PlayStation 3 can display HD content when the security flag (flag) is activated.

According to a statistic in the US market, by the end of 2006, there were about 16 million households with HDTVs but actually only about 7 million households fully exploited this feature.And among the HDTV owners, only about 51% have true HD support screens.25% of people watching television on HDTV via a normal cable are thinking of watching high-definition TV because the program starts playing with a stream of ambiguous messages that are a standard HDTV broadcast for the ready area "Broadcast in HDTV where available ".Finally, about 20% of users do not know that to watch HDTV, they need to have additional equipment.

Le Duy
Refer
www.atomicmpc.com.au
www.drmblog.com