The State of Digital Rights Management in Computer Games

Author: Connor Blanck

Email: connorblanck@gmail.com

Mentor: Ming Chow

Abstract

As early as some of the first commercial computer games, DRM or Digital Rights Management has been in place to avoid the illicit copying and distribution of software. While earlier DRM often made use of only off-disc copy protection like CD keys, more current DRM is more likely to make use of copy protection like online activation or verification, data position measurement as seen in SecuROM, or even the requirement of a constant online connection. Growing alongside the development of DRM and copy protection was the desire to bypass these protection systems to allow for people with pirated copies to play the game. This conflict has been a center of controversy as game developers attempt to balance the integrity of their software with the intrusive nature of some DRM schemes, leading to some eschewing copy protection altogether while others attempt to use the most restrictive copy protection to avoid lost sales. This paper will examine the software used in the most popular DRM technologies today, the software "cracks" that attempt to bypass them, and how most current models of DRM in video game software have failed to properly satisfy both the producers and consumers.

Introduction

DRM has become an increasingly prevalent issue in the video game world as the fanbase for gaming grows and the method of distribution increasingly shifts from physical DVDs to digital distribution. As systems of distribution become more complex, methods of controlling that distribution grew in a similar fashion. As a result, DRM has become much more obvious and intrusive in its mission to stymie software piracy with questionable rates of success.

What They Use

One method of copy protection involves actual physical media employing a method known as Data Position Measurement, essentially creating a CD or DVD fingerprint. This method of copy protection, employed by companies like SecuROM, essentially uses the CD/DVD physical medium to encode a cryptographic key that is used to decrypt the files within. The protection aspect of storing the key within the disc relies on the imprecision of average disc copying software and hardware to properly copy over the key in order to ensure the average pirate will not be able to bypass this protection. The implementation of this sort of copy protection is done entirely through the vendor e.g. SecuROM. In their case, they provide two options for for implementing the protection. [1] The first is to send your master disc directly to Sony DADC (owners of SecuROM) to have them apply the encryption and then replicate the disc for sale. The other option is to use their Online Encryption Toolkit (OETK) to encrypt the disc yourself, and then send the master disc to a replication plant licensed by SecuROM.

SecuROM is also known for using another type of copy protection that requires online product activation. This type of protection is notable for not requiring a physical disc for protection. It basically works by requiring the user to input a serial number associated with their purchase. Then, using information from the user's hardware, a unique id is generated for the particular machine that the software is being installed on. Both of these are sent to an external server where they are checked for accuracy and recorded after which an unlock code is presented to the user that can be used to decrypt the game files. [2] This DRM scheme discourages piracy not only by locking the software until the unlock code is received, but also by allowing the game companies to specify a certain number of activations allowed for a given key. In using this, companies are able to work around the fact that digitally distributed games are even easier to copy than physical media.

A third increasingly more popular option (as Steam's recent user concurrency milestones can attest to [3]) is the idea of always online DRM. Well known examples of this form of copy protection include Valve's Steam platform, Electronic Art's Origin system, and Blizzard Entertainment's Battle.net service. All three of these serve both as a method of distribution and a method of control, each requiring the user to login for at least a portion of time in order to access the games they have purchased or redeemed through the service. In many cases, like in the case of SimCity which was released earlier this year through Origin or Diablo III released last year, a constant internet connection to the service is required to use all aspects of the game, even the single player components. [4]

Why It Doesn't Work

The preceding technologies would be very helpful for game companies interested in curbing piracy if they actually worked. The unfortunate fact is that nearly ever DRM scheme, regardless of complexity or intrusiveness, will eventually be worked around by some Warez groups somewhere in the world. Even if it takes two years to create a proper cracked executable [5] or if it is cracked before it's even released [6], it's nigh on impossible to stop a group of dedicated individuals from getting access to something like a videogame that is distributed all across the internet.

For copy protection relying on Data Position Measurement, all that was needed to break it was advances in software's ability to properly record aspects of the physical media into an image file. This method of imaging is described in a patent filed by Dt Soft Ltd., who create the virtual drive and disc copying program known as Daemon Tools. [7] By measuring the execution times of disc reads and using calculations based on the physical geometry of a disc, it is possible to keep track of the actual position of data on the disc and store that information as part of a disc image. This same idea is used in another virtual disc/disc copying program known as Alcohol 120%, which even has an FAQ on their

support site on how to image a DVD protected by SecuROM. [8] This clearly reveals the inadequacies of this form of disc-based authentication, and further reveals that SecuROM's hopes of security through difficulty in copying probably aren't the most secure. Additionally, as evidenced by my email interaction with SecuROM support, the fact that they also utilize security through obscurity ("Our technology is proprietary and confidential" [9]) doesn't help their case either when it comes to robustness of solution.

Online activations have been similarly broken by Warez groups. In this case, it is not generally as simple as breaking protection that uses data position measurement, but it has clearly been done as evidenced by the incredible volume of cracked games to be found on the internet. One of the possible workarounds for this form of protection lies in the fact that the game eventually has to be decrypted in order to be playable. Once decrypted, even in the decrypted files are only stored in memory, it is possible to copy these files back into an executable that can be used to run the game. Then, it is a matter of looking through the assembly of the executable and removing or modifying the operations that actually call the authentication subroutines.

Dealing with always online DRM is probably one of the trickiest method of protection to break, as the constant online connection often carries with it data from the game developers' servers that contribute to the experience, as is the case with SimCity. SimCity's always online supposedly [4] uses the capabilities of EA's servers to do cloud computation to ease the load on a user's computer. Even this has been broken though. [10] In the case of SimCity, a separate server has to be run locally, with a modified hosts file that has EA's Origin servers instead being pointed to the local servers. Working around Steam's DRM is simpler in that it generally only requires a cracked Steam dynamic link library (dll) for that specific game in order to intercept API calls made to the Steam client.

Why The Consumer Loses

If it's been demonstrated that pirates can get access to a video game locked down with DRM by using a workaround or a cracked executable, then who actually ends up having to deal with the protection? It's the end user who legitimately purchased the game that really has to pay the price set by DRM. For on disc protection, this means constantly having to have the disc on hand in order to use the game, which can be an incredible pain especially if the disc goes missing. For off disk protection, the difficulties vary wildly. Activations and always online DRM require that external servers remain accessible and responsive in order to avoid delays in the consumer actually playing the game. As may seem obvious, this is rarely the case even when there is an understanding of the volume of players that will be attempting to authenticate. Just searching for "Diablo III Error 37" or taking a look at SimCity's catastrophic launch [11] shows just how painful DRM can be to the people who shouldn't even have to be aware of its existence. In addition, even if the servers are working, online activation limits introduce a limit on how many times a game can be installed, often on the same computer as well. If you decide to swap out memory or add another hard drive, it's possible that the computer won't be recognized as the one used during activation, requiring another activation to be wasted. It seems clear that you should be able to access the software you purchased, but in the world of DRM, this is frequently not the case.

To The Community

The issue of DRM in videogames is not one of trying to be on the cutting edge of security, or trying to keep a bad guy out of sensitive data. It's an issue of balancing consumer experience with software protection, and it's one that has been under addressed or dealt with in a horrible manner. Game developers understand that DRM doesn't really work [12], but there has been there seems to be

an incredible amount of misinformation on the ability of DRM to actually affect the piracy of games. To that end, it is critical that consumers get informed about the failures of current copy protection schemes and how this actually affects them. Additionally, it is important to find alternatives to these schemes that respect the consumer and acknowledge the inevitability of piracy.

Action Items

There are a couple ways that to fix the current state of DRM in computer games. The first is simply to remove DRM altogether from distributed software. While it may seem counterintuitive, vendors like the Humble Bundle [13] and GOG.com [14] have shown again and again that offering convenience and respect to the consumer will always beat out a game drenched in restrictions. If piracy is an inevitably, as has been demonstrated above, then it makes sense to treat the legitimate consumer as well as possible. This also saves money for the game companies because they don't have to spend money on SecuROM protection, or having servers that have to be constantly online. What is necessary for this shift is consumer education and a better understanding of the security flaws in current DRM for the publishers and developers who end up making the decisions on whether to include copy protection. If the illusion of security is too valuable to game companies that want to include DRM, then consumers need to keep track of who is using DRM, and vote with their money.

A second option to fixing DRM is to offer DRM as a service to the consumer in a manner similar to what Steam is doing today. While Steam's DRM is breakable, it removes the Steam benefits from the game, including an overlay that can be brought up to chat with friends, browse the internet, and access a community hub for the game. This is obviously a very good way to encourage users to buy a legitimate version of the game. Unfortunately, Steam falters in not allowing an offline mode that actually

works for all of their games., because it's possible that offline mode won't work at all if you shut down Steam incorrectly. [15] This alternative still requires that the DRM process is transparent and convenient, because if stealing the game and going through the steps (often many steps as with SimCity) to break the copy protection is more convenient than just playing the game, then there is a serious problem

Summary

There have been many methods employed to stop people from pirating games, but as has been clearly shown they rarely work. The real effect of copy protection is felt by legitimate consumers, who end up having to suffer the draconian DRM schemes implemented by game companies. In order to fix this problem, game companies and consumers should work together to improve the conditions of legitimate customers. Companies should consider removing DRM altogether or at least implementing DRM that works for the consumer, rather than against the pirates. Consumers should educate themselves on the flaws of the current copy protection security systems and spend wisely in order to not support the companies that force customers to suffer through the trials of overly demanding DRM.

References

[1] "SecuROM Disc Check." *SecuROM*. SecuROM, n.d. Web. 10 Dec. 2013. <https://www2.securom.com/fileadmin/user_upload/downloads/SecuROM_Disc.pdf>.

[2] "SecuROM Product Activation." *SecuROM*. SecuROM, n.d. Web. 10 Dec. 2013. <https://www2.securom.com/fileadmin/user_upload/downloads/SecuROM_Product_Activation.pdf>.

[3] Soper, Taylor. "Steam Hits 7 Million Concurrent Users for First Time, up 16% from Last Year." *GeekWire*. GeekWire, 1 Dec. 2013. Web. 10 Dec. 2013. <http://www.geekwire.com/2013/steam-hits-7-million-concurrent-users-time-16-year/>.

[4] Bradshaw, Lucy. "SimCity." *SimCity.com*. Electronic Arts, 20 Dec. 2012. Web. 10 Dec. 2013. <http://www.simcity.com/en_US/blog/article/The-Benefits-of-Live-Service>.

[5]"Assassin's Creed II-SKIDROW." *Skidrowcrack.com*. Skidrow, 11 May 2012. Web. 10 Dec. 2013. <http://skidrowcrack.com/assassins-creed-ii-skidrow/>.

[6] Houghton, Stuart. "Spore Cracked And Torrented, Already." *Kotaku.com*. Kotaku, 3 Sept. 2008. Web. 10 Dec. 2013. <http://kotaku.com/5045120/spore-cracked-and-torrented-already>.

[7] Naydon, Andriy, and Sergiy Naydon. Method of Storing Rotating Media Data in Image File. Dt Soft Ltd., assignee. Patent US 7463565 B2. 9 Dec. 2008. Web. 10 Dec. 2013 <https://www.google.com/patents/US7463565>.

[8] "Alcohol Soft Product Support." *Alcohol Soft Product Support*. Alcohol Soft, n.d. Web. 10 Dec. 2013. <http://support.alcohol-soft.com/knowledgebase.php?postid=24649>.

[9] SecuROM Support. “[Ticket#2013102910000929] SecuROM technology” Message to Connor Blanck. 31 Oct. 2013. E-mail.

[10] "Maximus" "How to Install SimCity (2013) (Bypass DRM/Play Offline)." *Pathetic Reviews*.

Pathetic Reviews, 12 June 2013. Web. 10 Dec. 2013.
<http://patheticreviews.com/2013/06/12/how-to-install-simcity-2013-bypass-drmplay-offline/>.

[11] Peterson, Steve. "Will Wright: Games "falling Way Short" as a Medium." *GamesIndustry.biz*. Gamesindusty International, 6 May 2013. Web. 10 Dec. 2013.
<http://www.gamesindustry.biz/articles/2013-05-04-will-wright-games-falling-way-short-as-a-medium>.

[12] Klepek, Patrick. "CD Projekt RED Waves Goodbye to DRM." *Giantbomb.com*. Giant Bomb, 11 Nov. 2013. Web. 10 Dec. 2013.
<http://www.giantbomb.com/articles/cd-projekt-red-waves-goodbye-to-drm/1100-4783/>.

[13] "Humble Bundle." *Humblebundle.com*. Humble Bundle, n.d. Web. 11 Dec. 2013.

[14] "GOG.com." *GOG.com*. GOG.com, n.d. Web. 11 Dec. 2013.

[15] "Offline Mode." *Support.steampowered.com*. Steam, n.d. Web. 11 Dec. 2013.
<https://support.steampowered.com/kb_article.php?ref=3160-agcb-2555>.