How Effective is Computer Game Copy Protection?

Computer game piracy offers lessons for the rest of us on data leakage protection.

BY RICHARD HYAMS AND PETER WILD

Royal Holloway University of London

How Effective is Computer Game Copy Protection?

Richard Hyams
Information Security Manager, SCI Entertainment PLC

Professor Peter Wild
Information Security Group, Royal Holloway, University of London, Egham, Surrey, U.K.

Today's video games industry generates huge profits. A popular computer game such as Microsoft's Halo 3 can earn as much as a top box office release in a weekend.

US computer game sales in 2006 reached $7.4 billion, but it is estimated that the industry lost more than $1.9 billion to global piracy, and piracy is on the increase. The games is actively seeking mechanisms for preventing unauthorised copying and distribution.

Protecting a game from being copied is most effective during the first 6-9 weeks from its release date as this is when the majority of sales occur. Any illegal copying after this period will have a lesser impact. The second-hand market for computer games has developed in which pre-played games are "recycled". Many computer game retail stores have set up facilities to buy back games to resell them. Game developers and publishers do not generally receive any sales revenue from this market but it has the effect of reducing sales of full-priced games, as gamers will buy the cheaper second hand one. The development of the secondary games market has added a new twist and may possibly require the game to be protected longer to delay it being resold.

BULLETIN BOARD SYSTEMS

Computer games have always been illegally copied. The first community Bulletin Board Systems (BBS) made it possible to exchange pirated copies of games with lots of people, and although not all BBSes were setup solely to exchange pirated games, a significant underground "scene" emerged where groups of people would exchange electronic files between them. BBSes cost money to run and so special "paid for" accounts were setup for people not in the hacker community to have access to the cracked software. BBS operators however were running a big risk. Unlike websites, the computers running the BBS were based at the system operator's home and could be traced by the police. For this reason the "scene" was very secretive, with phone

This article was prepared by students and staff involved with the award-winning M.Sc. in Information Security offered by the Information Security Group at Royal Holloway, University of London. The student was judged to have produced an outstanding M.Sc. thesis on a business-related topic. The full thesis is available as a technical report on the Royal Holloway website http://www.ma.rhul.ac.uk/tech.

For more information about the Information Security Group at Royal Holloway or on the M.Sc. in Information Security, please visit http://www.isg.rhul.ac.uk.

numbers and names traded between people that knew each other and new members even being voting on by existing members of a BBS.

Microsoft, Novell and other large corporations became so concerned that they worked with the FBI to try and close the BBSes down. In 1997, "Operation Cyberstrike," run by FBI's international computer crime department in San Francisco, shutdown five major pirate BBSes in one week and caused many others to shutdown in fear. New anonymous methods of distribution over the internet began to be used by the hacker community. IRC channels were originally used, which then evolved into using Peer to Peer networks (P2P) such as BitTorrent, Emule and kazaa. With the emergence of the large search engines it became very easy for far more people to find pirated games than by the old secretive bulletin boards. A search (for example, on Google) will find almost any pirated version of the latest video games. Some dedicated "torrent search" sites have sprung up to help users locate pirated torrent files more easily, such as Sweden's "Pirate Bay".

The computer games industry has tried to prevent illegal copying by firstly preventing the game CD from being physically copied by a CD recorder and secondly preventing the game code from being transferred from the CD to the hard disk. Many methods have been tried in the past. These range from altering the physical structure of a CD which prevented the use of early CD-copiers, to random words from an instruction manual having to be entered during the game start up requiring the manual to be copied.

ENCRYPTION

Most of these methods were either too expensive, incompatible with existing computers, or were broken by the hacker groups. The main method that emerged over time was encryption. The game code is encrypted on disk and has to be unencrypted before the game can be played. It may seem at first sight, that the hacker would have to attack the encryption to make a copy, but as the game has to be unencrypted to be played the hacker can wait until it is unencrypted in the computer memory and attempt to copy it from there. A game of cat and mouse began between the developers and the hacker groups as more and more sophisticated mechanisms based on the encryption idea were developed and subse-

A game of cat and mouse began between the developers and the hacker groups as more and more sophisticated mechanisms based on the encryption idea were developed and subsequently cracked.

quently cracked.

Computer games are still mainly distributed on physical media such as CDs and DVDs but the general availability of broadband connections makes it possible to download entire computer games. Although the number of sales are small compared to traditional retail, they are beginning to increase as more game consoles are now able to connect to the internet. It should be noted that increased bandwidth has also helped the hacker community who can now distribute entire pirated games rather than just the program to crack the copy protection.

DIGITAL RIGHTS MANAGEMENT

Online distribution of games, just like digital music, has introduced the use of digital rights management (DRM) as a new method of copy prevention. DRM originally focused on security and encryption, and tried to lock content down to just the user that originally bought the computer game. As the online computer game market evolved, a second generation of DRM was developed which, instead of preventing direct copying, stopped the game from being played without some form of registration. This is done by an "online" account which forces the purchaser of a computer game to validate the game via an online platform. The DRM tries to prevent a user registering and using a pirated copy of the game. Thus, the user may have the software but be unable to run it. This type of DRM is less focused on encryption and more on the monitoring and identification of a game with its associated online account. The best examples are Steam, which was developed by Valve Corporation the developers of the popular Half Life 2 game, and Microsoft XBox-Live, which connects Xbox 360 consoles to a managed multiplayer platform.

Unlike digital music or films, computer games have the potential to be upgraded with new levels, maps and additional weapons, and this creates an incentive for a user to continue an online relationship with the games developer or publisher. Success stories, such as the hugely successful online universe "World of Warcraft," have proven that subscriptions models work. Game activation and linking to an online account can be repeatedly performed over a given period or every time the game is played. This gives the DRM an ongoing control system to identify illegal licences and delete the accounts instantly. Although a user may have success-

Online distribution of games, just like digital music, has introduced the use of digital rights management (DRM) as a new method of copy prevention.

fully registered an unlicensed copy of a game when they first installed it, at any time the illegal licence may be detected and the account disabled.

Just cracking a game's copy protection code is not sufficient any more. This is in contrast with retail games played offline which, once cracked and distributed on the internet, allow many users to play the pirated software. Copy protection linked with online accounts may seem to be a formidable step against the hacker groups but they really work best when the game has a multiplayer option. The incentive to keep the consumer legal is the threat of being banned from a multiplayer platform.

Single player games will probably still be cracked, as shown by Half-Life 2 which was cracked but only worked in single player mode. The potential problem is that if an online account is stolen then the legitimate user's game copy as well as the pirate one could be banned, so there needs to be a process to allow the legitimate user back on but stop the pirate copy from returning.

Another avenue of attack is to target the multiplayer platform itself. An example of this is the online platform called Battle.net developed by Blizzard Entertainment, which like Steam, validated a user's licence before allowing access. A group of hackers reverse-engineered the protocol language used for communicating between the game and the online platform. This meant they could set-up their own online Battle.net environment with the account disable functions turned off and allow users with pirated copies to play.

ONLINE ACCOUNTS

In future, games developers will almost always include multiplayer options in their games, thus enforcing a connection between the consumer and the developer. The developer now has many more options then ever before to control who plays and on which device. As Microsoft Xbox Live and Steam have shown, it will become much harder to bypass the control mechanisms and involve much more effort from the hackers such as producing their own rival online platforms. In the long term the home computer will evolve into the media centre of the living room. Buying games may be like watching an on-demand movie with the same type of rental business model. Games will no longer be for sale on physical media and as online technology develops, it may be that

Copy protection linked with online accounts may seem to be a formidable step against the hacker groups but they really work best when the game has a multiplayer option.

only the part of the game being played will be available on the device at any one time.

Will there ever be a perfect copy prevention solution for games? Online accounts look the most promising, but there will always be a race between the games developers and the hacker groups, and it is usually only a question of time and motivation before the protection is broken or bypassed.*

Ron Condon

UK bureau chief
searchsecurity.co.UK

Ron Condon has been writing about developments in the IT industry for more than 30 years. In that time, he has charted the evolution from big mainframes, to minicomputers and PCs in the 1980s, and the rise of the Internet over the last decade or so. In recent years he has specialized in information security. He has edited daily, weekly and monthly publications, and has written for national and regional newspapers, in Europe and the U.S.