The Effects of Software Piracy on Consumers and Software Developers

By Adam Leinss
For CS-699 Independent Study under Dr. Levine

The History of Software Piracy

The history of software piracy dates back almost to the invention of the consumer computer itself. Software piracy began when Ed Roberts created a company called the Micro Instrumentation Telemetry System (MITS). Soon after the creation of the company the Altair 8800 was created. The computer was first published in the January 1975 issue of Popular Electronics. The basic kit was $397 and was geared toward hobbyists and required much assembly on the user's part. Shortly thereafter Bill Gates and Paul Allen saw the magazine ad and persuaded Roberts to license BASIC, a programming language from them (Rue, 1990).

In June of 1975 MITS started marketing the Altair via a national tour. They would set up the Altair computer in hotel seminar rooms and invite people to see the low priced computer running various programs. When MITS stopped in Palo Alto, California, the Homebrew Computer Club was there to see the Altair and saw it was running BASIC. Many of the hobbyists had ordered BASIC from MITS, but it had not been released publicly as "bugs" were still being corrected in the code. Someone then borrowed one of the paper tapes lying around that contained the current version of BASIC and later gave it to Dan Sokol, who was a member of Homebrew Computer Club. He wrote a program that copied the punch card pattern and thus became the world's first software pirate (Rue, 1990).

Piracy continued with the introduction of the Apple II computer in 1977. Steve Wozniak was the creator of the Apple II. He was also a member of the Homebrew Computer Club, the same club that Dan Sokol belonged to. Steve Wozniak was well aware of software piracy as demonstrated from his speech to the Apple World convention in 1986:

"*...I do not believe that it costs software publishers one cent...You can believe what you want to believe, but it's hard to say that anyone with $20 a month in allowance money is going to buy $150 pieces of software. They might have copied it, but they did not steal $150, because they could not have afforded to buy it. The resources weren't there. Just a viewpoint of mine."* (Connick 24).

The Commodore 64 hit the market in September of 1982. By the end of that year, there were already groups of people removing the copy protection from games. One of the first games for the Commodore was "Commodore Soccer" which was cracked by a German man called "1103". Distribution of pirated software was limited mainly to elite hobbyist groups via hand and mail delivery and connections between two computers using a modem at the speed of 300 baud (30 bits per second). To remain anonymous, most groups used P.O. Boxes. There were bulletin board systems (BBS) in existence during this time. A user with a modem could dial in to a BBS to upload files so that multiple people could dial in afterwards and download the uploaded files. However, storage space during this time was limited and most calls were long distance which would make transmitting programs via BBS' very expensive (Walleij).

The IBM PC pirating scene did not begin until the late 1980s even though the IBM PC came out in 1981. Many warez (underground term for illegal software) groups were still using Amiga and Commodore computers during this time. Most of the groups that started the IBM piracy ring were from the Amiga and Commodore era. Razor 1911 (which was founded in October of 1985) officially started releasing IBM software in 1991. Around this time the National Science Foundation lifted the restriction on commercial use of the Internet, clearing the way for the age of electronic commerce. This opened the flood gates for software piracy. Users starting offering pirated software on various venues of the Internet such as USENET, IRC (Internet Relay Chat), and FTP (File Transfer Protocol) sites. USENET is an international massaging board where one user posts a message to a news server and then that server propagates the message to other news servers around the world. In addition to text messages, users could also post binary files and thus the birth of piracy over USENET was born. In fact, at the present time, one can find many pirated software titles including every Microsoft title ever made on USENET. 200 gigabytes of data per day are currently passed through USENET making investigation of the people posting pirated software a very difficult task.

IRC was and still is another popular venue of software pirates. There are various IRC networks around the world such as EFNet, UnderNet, DalNet, etc. On these servers, there are thousands of channels. Any one can make a new channel on these networks. Software pirates opened their own secret chat channels to distribute files and to hold meetings with their respective members. The channels can be made locked in that only people knowing the password can get in or the channel can be hidden from the channel list, thus someone only knowing the exact channel name will be able to "find" the channel and enter it. FTP sites are also a favorite place of software pirates. Using special scanning programs pirates look for public FTP sites that allow uploads and download of binary files. Once a pirate finds a viable site (i.e. one that is fast and people can both upload and download from), the pirate will make a secret directory and then transfer the pirated software into this directory. After doing so, he or she will usually let the other members of the warez group know where the files are so that they may download them and distribute them to other places (e.g. IRC or USENET).

In 1994 a landmark case dealing with software piracy came to the surface. David LaMacchia, a 21 year old student at MIT, operated an Internet site that allowed users to upload and download pirated software. Because he sought no profit from his actions, actions that caused substantial economic harm to software companies, he could not be charged under the criminal provisions of the copyright law at the time. The United States District Court dismissed an indictment charging LaMacchia with wire fraud on the ground that his acts did not violate the wire fraud statue. This case became known as the "LaMacchia Loophole". Soon after case, Congress passed the NET act (No Electronic Theft) in November of 1997. Under this legislation, anyone distributing copyrighted works with a total retail value of more than $1,000 within a 180-day period could be fined and imprisoned for three years (for the first offense) and up to six years for subsequent offenses. Thus, the "LaMacchia Loophole" was closed (Grabosky 100).

In December 2001 a large raid by FBI took place. U.S. agents seized computers in 27 American cities. The operation (called Buccaneer) targeted one of the oldest pirate rings called DrinkOrDie (DoD). Founded in Moscow in 1993, DrinkOrDie became famous among software pirates when it released a copy of Microsoft Windows 95 two weeks before the program went on sale. No arrests in the U.S. were reported at the time (Grabosky 100).

New anti-piracy technologies, encryption and laws will likely not stop piracy. The battle between the software companies and the pirates will simply continue. The Internet is by nature lawless and designed for the free exchange of information, with an emphasis on the 'free'. As long as there's a market, there will be a black market.

The Software Industries' Various Methods of Combating Piracy

There are various methods of combating piracy. One of the main methods is providing protection within the software itself. One of the most common is serial number protection. The basic serial number protection involves just entering in a valid serial number and nothing else. For example, to register Real Player Plus, a media player, one only needs to input a valid serial number. The serial number is not tied to the registered user's name. In other schemes the serial number is derived from the registered user's name. In this way the user is less likely to give out their key to someone else or put it on the Internet. More advanced schemes involve generating numbers based on a hardware hash. The program uses an internal algorithm based on various hardware components in the system (e.g. CPU and motherboard type) to generate a unique "computer id" for that specific computer. The user then must use this "computer id" in their registration process. The company of the software product then uses another piece of software with another algorithm that uses the customer's "computer id" to generate a serial number. No matter how the complex the serial number protection is it can always be broken or "cracked".

A famous case of this came out in 1996. iD Software decided to release a shareware CD for $10 wherein the user could play one level of each game. The full versions of the games were on the CD encrypted using the technology provided by the TestDrive company. The encrypted, full version software on this CD included titles such as Quake, Hexen, Doom 2, Final Doom and Wolfenstien 3D just to name a few. In order to unlock the encrypted titles the user would run the QSTART.EXE program. This program then brought up a menu wherein the user could pick which title he or she wanted to "unlock". The TestDrive program would then generate a key 12 digit "computer id" code. The user, if he or she really wanted to buy the game, would then call 1-800-IDGAMES. The user would then give this "computer id" code to the customer representative. The customer representative would then plug this "computer id" into their software and it would generate an unlock code. The user could then plug this unlock code into the second box (under the "computer id" box) and have the full version of the game. In October of 1996 a cracking group called GNOMON introduced a key generator (usually called a "keygen" in the underground). This program could make valid unlock codes based on the "computer id" code that the QSTART.EXE created. It meant that the

$10 shareware CD-ROM that iD Software was distributing was now worth $370, because anyone could unlock the games for free on it. The encrypted games were also being distributed at www.testdrive.com/idout, but were quickly removed after the key generator was discovered (Bruyn).

Another form of copy protection technique is provided by dongles. A dongle is a hardware device that connects to the printer port, serial port or USB port on a PC. When the protected application starts it checks to see if the correct dongle is in place. If it is not, the program will not function. For added protection, all communications between the software application and the dongle are encrypted by uncrackable algorithms. Internal security fuses in the dongle ensure that any attempt to hack the dongle mechanically causes it to self-destruct. Dongles are mainly used for specialized applications that typically have higher pricing. "*The dongle may be called every 150 mouse clicks, or each time you print, or if you select flesh tones as your desktop color scheme*," reports one dongle expert. The biggest producer in the dongle market is Rainbow Technologies whose Sentinel hardware keys are used by 55% of all protected software. There are 8 million Sentinel dongles attached to 8 million machines the world over. The company calls it: "*the world's most effective way to stop piracy*" (McCandless 177).

The logical approach to cracking dongled software is to create a "pseudo-dongle", that is a software program pretending to be the hardware dongle and giving the correct answers to any query coming from the protected application. Theoretically, to construct this fake dongle, the cracker would have to monitor and trap information passing between the computer and the dongle to build an infallible query and response table. Unfortunately, if the query is sufficiently large, it will be impossible to duplicate. For example, assume the query is 6 characters long. Then it can have over 280 trillion possible responses. With modern machines, this would take around 44,627 years to compute. With Rainbow's SentinelSuperPro dongle the query length can be up to 56 characters requiring 10^{125} years of computing for a complete query and response table (McCandless 177).

The SentinelSuperPro dongle attached to Kinetix 3D Studio Max 2.0, however, was cracked in just under seven days of its retail release by ForceKill of leading warez group DOD. Other expensive applications that use Sentinel (NewTek's Lightwave, Microsoft's Softimage, and Autodesk's AutoCAD to name a few) have also be cracked and distributed on the Internet. Instead of attempting to simulate the dongle, expert crackers simply remove the dongle checking from the program code by examining the relationship between the protected software and the dongle function by function and call by call, until the application ceases to need the dongle to function at all (McCandless 177).

Sometimes there is copy protection on the CD media itself. When CD burners became popular in the mainstream market, software makers realized that they need to prevent duplication of their programs. One of the most popular CD copy protection schemes is SafeDisc. The SafeDisc technology is a software-based solution that does not require any changes to standard PC or CD-ROM hardware. It is comprised of both an

authenticating digital signature embedded on the disc, as well as a multi-layered encrypted wrapper that secures the CD-ROM content. The digital signature, which cannot be copied by CD recorders or mastering equipment, is embedded by the laser beam recorder at the time the CD-ROM master is made at the mastering facility (CD Protection).

The SafeDisc technology, however, has been broken by software pirates. When you play a game that is SafeDisc protected it checks to see if it can find the embedded serial number on the disc. Once it finds this serial, it decrypts the game executable from the ICD file on the disc and runs it. Sophisticated software pirates have circumvented this process by dissembling and extracting the game executable out of the ICD file directly. In addition to the SafeDisc technology, many manufacturers also put unreadable or invalid sectors on the disc to confuse CD-ROM burners and thus preventing them from making a copy. Pirates have gotten around this by using special programs such as BlindWrite and CloneCD and high-end CD-ROM burners to make near perfect images of these discs (CD Protection).

Software Companies Monetary Losses due to Software Piracy

Software pirates can destroy the revenue stream of small companies that have successfully found a niche in the industry. Without this revenue stream, these small companies lack the resources for development of new software innovations which decreases the chances of making a profit. The inevitable result is that these small companies often become economically unstable and often "go under," all because software pirates have decided to steal their software and make it available to others (SIIA 13).

Revenues Lost to Software Piracy by Region

(thousand U.S. dollars)

	1997	1998	1999
Western Europe	$2,519	$2,760	$3,630
Central Europe	561	640	409
North America	3,074	3,196	3,631
Latin America	978	1,045	1,128
Asia/Pacific	3,916	2,955	2,792
Middle East	206	190	284
Africa	186	190	194
WORLD TOTAL	**$11,440**	**$10,976**	**$12,163**

Figure 1. Revenues Lost to Software Piracy by Region (SIIA 3)

In addition to piracy problems, the copy protection schemes themselves can be expensive. Dongles are not an option for many software companies since they add an additional manufacturing expense of between $5 and $20 to each copy of the program. Dongles also do not facilitate Internet based distribution of software since a dongle must be shipped to each customer to allow operation of the software. In addition to the expense, copy protection can drive users away. Bob Lentini of Innovative Quality Software, maker of the SAW (an audio program) says the following:

"*We don't use copy protection on any of our current products. It has been my experience that in the long run the pirates do not cause as many lost sales as you might expect. Those of the pirate mentality would never have purchased the product anyway if they could not steal it. Many of our customers came to us after running a pirated version for a short time, and then decided that they could not live without the product and wanted to register for access to support and free downloads and other product discounts. Others have purchased after seeing a pirated version running in some other location...free advertising*" (Winer).

Complicated copy protection puts an unneeded strain on end users and in some instances it can actually hurt a company's performance. This is demonstrated by Todd Souvignier, Marketing Director of Arboretum Systems:

"*As we're about 75% Mac, when we learned that Apple was eliminating the floppy drive, we saw the writing on the wall, held our breath, and got rid of the key disks and dongles in one fell swoop last fall. Surprise! Our product sales actually increased. Not only that, our tech support calls were cut by two-thirds, and our cost of product manufacturing was cut in half. So I'm a serial number-only believer. I hate challenge / response schemes. Making the customer wait upwards of a day or more to run their new purchase is intolerable*" (Winer).

Effects of Software Piracy on Users

Experts say that pirated software often includes incomplete or damaged programs, which can function incorrectly or hurt productivity. Consumers using illegal software generally cannot get access to product support, instructional materials, or low-cost product upgrades. Businesses using illegal software are subject to legal action, fines, and low productivity. In addition, experts say that pirated software can also include computer viruses which can destroy data on a user's hard drive. "*Computer viruses can have a devastating impact on any computer user -- from the home user to a large business*," according to Larry Bridwell, virus expert at the National Computer Security Association. "*One of the best ways to avoid computer viruses is to only use legitimate software from reputable sources. Using pirated software is an open invitation for computer viruses*" (Smiroldo).

Companies can also be subject to raids by the SIIA. The SIIA raid begins with an informant. Informants are anonymous and often include disgruntled employees. Both the

SIIA and BSA have toll-free anti-piracy hotlines that alert them to piracy violations. The SIIA receives about 30 calls a day, but only 5 or 10 cases are pursued each week. Once the SIIA has been alerted to the problem they begin research. They find out how many software copies are being used and how many are registered. If there is a discrepancy in these numbers then legal action begins. The SIIA will send a voluntary audit request letter, and if the company does not comply with the voluntary audit, then they will be forced into a non-voluntary audit. A non-voluntary audit is more like a raid. The SIIA, assisted by federal agents, will show up unannounced and begin going through all of the computers on the property looking for illegal software. If pirated material is found, SIIA will prosecute. Lawsuits are highly publicized and result in large fines of up to $250,000 per infringement. In 1996, after a raid by the BSA, Utica Enterprises agreed to pay $260,000 in fines, delete the illegal software, and purchase software in place of it (Boulton 34).

Sometimes, however, companies can be wrongfully accused by the SIIA. Four armed U.S. marshals and three representatives from the SIIA arrived at the headquarters of Snap-on Tools Corporation in Kenosha, Wisconsin with a search warrant in March 1991. After spending the next two days printing out directories on all the firm's 300 computers, the SIIA asked the company to provide documentation conclusively proving that the software listed in the directories was legal. "*It was worse than getting audited by the IRS*," says David Heide, a public relations manager who was present at the time of the raid. "*At least the IRS sends a letter of notice that it's coming*," he adds. Snap-on suffered legal costs, operational costs of having computers occupied by SIIA officials, and the public humiliation due to the raid (Radding 42).

The SIIA actions were also questionable when they took action against a small newspaper publisher BHG Company, when they brought a charge of $120,000 in fines (two-thirds of BHG Company's annual gross revenue) for using illegal copies of Adobe Photoshop and Adobe Pagemaker. Hundreds of papers in neighboring areas offered to run anti-piracy ads and the settlement was reduced. Most SPA actions result in fines. Jail time, although rare, is the worst punishment of all. Jeffery Solocheck was a software reseller who served a one-year prison sentence while his family of three awaited his return. While admitting to perjury, he claimed that he was innocent of the crime of piracy. Solocheck was convicted of piracy, and was sent to jail (Fitzgerald 6).

In addition, copy protection can create a nightmare for users. Most users hate dongles for a variety of reasons. Dongles can be troublesome to install and use since they often require a special hardware driver, and they can interfere with the use of peripherals such as printers and scanners. Since no standard exists for dongles, each protected program requires an additional dongle, which causes an unwieldy "pile" of connected dongles on the back of the PC. Ethan Winer has this to say about copy protection:

"*Any copy protection scheme that requires intervention from the publisher has the potential to cause you disaster. Suppose you're working on a project and your hard disk fails. So you go to Staples and buy another, only to find that your Key disk is no longer readable or it reports that you already used up your two allowable installations. Even the*

seemingly benign method of calling the vendor for an authorization number is a burden if you're working on a weekend and can't reach them on the phone. Or suppose the dongle simply stops working? You're in the middle of a project with a client paying $200 per hour, and you're hosed because even with overnight shipping: the new dongle won't arrive until tomorrow."

More recently, Microsoft included sophisticated copy protection in their operating system for the first time. In order to use Windows XP after 30 days, the user must activate their copy of Windows XP either by phone or the Internet. During the activation progress, Windows XP takes a "snapshot" of the user's system and generates a hardware hash value. Based on the key that comes with the CD key and the hardware hash, Microsoft will then activate the copy of Windows XP. There are several checks built-in to Windows XP that track if hardware is changed. If a user changes too many hardware components on their system then they will have to reactivate their copy by explaining over the phone to Microsoft why they need a reactivation of their copy. Needless to say, this has upset many users especially when an "Enterprise" copy of Windows XP that has no activation code in it at all has been leaked on the Internet by the warez group named Devils0wn. It seems that the only users that are affected by product activation are legitimate users.

About 5 months after the release of Windows XP, a keygen was released by the warez group called "The Blue List." The program generates random valid CD keys for the latest versions of Microsoft's products such as Windows, Office and Visio. The program sits in a continual loop and generates random CD keys based on how many the user requested. Not every random CD key can be activated, so it usually needs more than one try to compute CD key that can be activated (chances are about 1 in 40). In general it takes about an hour to come up with a usable CD key.

Product activation is also included in Office XP. About month before its official release, someone obtained a copy of the corporate version of Office XP which does not require an activation key, and posted it on the Usenet newsgroup alt.binaries.warez.ibm. What is surprising is what Lisa Gurry, product manager for Office had to say about this:

"*The activation technology was developed to prevent against casual piracy, and that is typically piracy when a consumer shares their software with someone else outside the terms of the licensing agreement. We don't think most of our users will be out on the Web trying to find ways to steal software*" (Patrizio).

It seems that Microsoft is not trying to prevent piracy between pirates, but between users themselves, even though Internet piracy costs them substantially more in revenue. Legitimate users are punished for other's misdeeds.

In the end, software piracy is both bad for the software industry and users. However, the cure (copy protection) seems to be worse then the sickness (software piracy). In many cases, all the copy protection does is prevents legitimate users from using the software. After 20 years, the number of pirated software titles continues to increase despite the advances in copy protection. Instead of spending countless dollars

on copy protection, the software companies should be looking at ways to track down software pirates and prosecute them and not punishing legitmate users.

Works Cited

Boulton, Sandy. "Software Pirates Walk the Plank." Mechanical Engineering January, 1996: 34.

Bruyn, Greg. A Keymaker for the Testdrive Registration System. November 1996. 3 Jan. 2002 <http://groups.google.com/groups>.

"CD Protection" CDMediaWorld.com January 2002. 9 Jan 2002 <http://www.cdmediaworld.com/hardware/cdrom/cd_protections.shtml>.

Connick, Jack. "And Then There Was Apple." Call-A.P.P.L.E October, 1986: 22-27.

Fitzgerald, Mark. "Small Publisher, Big Victory." Editor & Publisher February, 1999: 6.

Grabosky, PN., and Smith, R. Crime in the Digital Age. New Brunswick, NJ: Transaction Publishers,1998.

McCandless, David. "Warez Wars." Wired April, 1997: 174-181.

Patrizio, Andy. Pirates Experience Office XP March 2001. 11 Jan. 2002 <http://www.wired.com/news/business/0,1367,42402,00.html>.

Radding, Alan. "Companies Scared Straight by SPA Anti-piracy Raids." Infoworld Janurary, 1993: 43.

Rue, Timothy Vincent. SPONSOR-WARE: The Fading of Software Piracy. August 1990. 9 Jan. 2002 <http://www.mindspring.com/~timrue/sponsorV2.html>.

Software & Information Industry Association (SIIA). SIIA's Report on Global Software Piracy 2000 June 2000. 10 Jan. 2002 <http://www.siia.net/piracy/pubs/piracy2000.pdf>.

Smiroldo, Diane. "Congressional Hearings to Target Software Piracy." PR Newswire 24 Jun 1997.

Walleij, Linus. Copyright Does Not Exist. 1994. 3 Jan. 2002 <http://home.c2i.net/nirgendwo/cdne/mainindex.htm>.

Winer, Ethan. Copy Protection: The Audio Industry's Dirty Little Secret August 1999. 10 Jan. 2002 <http://www.prorec.com/prorec/articles.nsf/files/739DF48C566E1D33862567DE001BE355>.