‘MODDING’ OF VIDEO GAME CONSOLES

By Jeff Baxendale, Raphael Mun, and James M. Selevan

INTRODUCTION

The field of Information Security today is often used interchangeably with Internet Security. This is because many of the issues and vulnerabilities relevant to computers are involve the internet and insecurities in applications accessing the world-wide-web. In the world of video games, however, Information Security and protection of Intellectual Property (IP) take on a very different meaning in that the users are not the ones at the greatest risk but rather the corporate providers and the game developers.

While internet hacking and exploiting backdoors within operating systems are not easy feats, they represent a wide spectrum of issues such as national security that cannot be solely described as a highly profitable business in the way that video game hacking and game piracy mostly do.

From “legitimate” hacking/cheating devices such as GameShark and Action Replay that enable rare items and infinite money within video games, to the integration and sale of mod-chips that allow cheap, pirated copies of video games to be played on game consoles - security has taken on an entirely new type of warfare in the video game console market.

BACKGROUND HISTORY

INTRODUCTION OF CONSOLE EMULATION

In the 1970s and 1980s, video game consoles were just beginning to migrate into the homes from large arcade machines, through the Atari and the Nintendo Entertainment System (NES). These machines were highly specialized with their hardware to run programs (ROMs) manufactured on cartridges as efficiently as possible. Unlike the PC where software duplication was much easier, the concept of protecting these ROMs just did not exist as the production of game cartridges was tightly controlled.

Within a decade, as computers were growing increasingly powerful than the consoles, the emulation scene began to take shape as the hardware for various arcade and console games could be simulated with highly-optimized code on the PC. Digital forms of the cartridges, ROM "dumps", enabled any household PC to play video games without the purchase of the game or the console system itself. As timing would have it, technology allowed to anyone with access to the internet through their 56K dial-up modems to download these ROMs for free on the web. Even worse for the companies, as is with most new technologies, no laws were yet designed to protect them.

Video game emulation, however, was still a fairly small community consisting of mainly curious developers that simply wanted to push the technical limits of the PC with sometimes highly unreliable results. But one note-worthy emulator blasted through during this time called NESticle that provided unprecedented compatibility and a highly customized graphical user

interface. Its release created interest among many people that wanted to re-live the experience of the NES game system, were bored at work, or just never purchased video games. This breakthrough was the beginning stages of video game piracy and widespread distribution of ROMs.

ULTRAHLE AND HIGH LEVEL EMULATION

The next major breakthrough arrived soon afterward in January of 1999 with the release of another emulator called UltraHLE, named for its "High-Level Emulation". This emulator's design brought a complete change in emulation paradigm. Previous emulators were required to emulate all parts of the hardware from its low-level CPU operations to the RAM, interrupts, and all other low-level interactions. This type of emulation proved incredibly tedious to implement and debug. Development for this type of emulation could take well over a year to run correctly and perform at a playable speed along with the general requirement that the emulating system would need to be at least ten-times as powerful as the emulated system.

UltraHLE on the other hand, after just about a month of development by two people, was released for the latest generation console during its time, the Nintendo 64, only three years after the console was introduced (the average console generation lifetime is around 5 years). Unlike previous emulators, UltraHLE intercepted C library calls in the compiled code and simulated them on the native hardware. Because the number of library calls were much fewer than emulating the full number of CPU opcodes and other hardware details, the speed of development and the fact that it could run several of the most popular games put companies like Sony and Nintendo in full panic even if high level emulators were less compatible. Because

the libraries themselves were intercepted, opportunities arose for emulators to add effects and run the games even 'better' than the native system. Two emulators released for Sony's Playstation console following the HLE model, Bleem and Connectix, provided higher resolution and filtered textures that made the games appear smoother on the computer and brought on another round of emulation panic.

Video game security for the most part before the 21st Century was emulation and ROM-related. Legal-action threats were made to emulator authors and hosting websites, and the co-authors of UltraHLE, RealityMan and Epsilon, went into hiding after the fiasco; RealityMan, Gordon Hollingsworth, moved to Canada soon after and retired from the emulation scene.

THE IMPACT OF SEGA'S DOWNFALL

The last big security catastrophe in video game consoles was in 2000 involving one of the three mainstream console companies at the time, Sega Entertainment, and its Dreamcast system. While the console system itself was widely praised and grew to be rapidly popular among gamers as the first 128-bit console with supreme graphical capabilities and processing power along with broadband networking, the console silently faded into the background and was pulled after three years. While Sony's announcement of its competing console, Playstation 2, is credited for the Dreamcast's failure to gain momentum, other critics believe its lack of sales and failure was due to software piracy.

The Dreamcast used a special type of disc format known as GD-ROM that held about a gigabyte of storage not commonly sold at stored like the CD-ROM. This proprietary drive paired with revolutionary security measures implemented through software instead of hardware, was

expected to ward off video game piracy. However, a backdoor in the mask-ROM BIOS discovered by a German hacker group allowed the Dreamcast to boot normal CD-ROM discs without any hardware changes, and by minimizing data on GD-ROM discs to fit on the smaller CD-ROM, pirated games could be simply burned onto discs at practically no cost.

This security flaw not only encouraged piracy and discouraged sales of actual games, game developers for the Sega Dreamcast pulled out of the losing market for more profitable consoles. This failure of the console generation drove Sega out of the console business and became the biggest lesson in security for companies in the next console generation. Drastic new measures were taken by the Nintendo, Sony, and Microsoft to battle video game piracy.

Business and Market Issues

While it is mostly a recent occurrence that the games industry (and especially the PC games industry) is concerned about consumer software piracy, some of the first forms of console DRM dated back to the original Nintendo Entertainment System.

10NES Chip

Nintendo originally designed a form of cartridge protection called the "10NES" chip. This served as a sort of lock and key mechanism for the NES to play games - for games to boot and run this verification process had to pass. Nintendo created this chip as a means to protect their royalties. The NES was owned by Nintendo and to develop games for the system one had to pay Nintendo royalties. Nintendo owned both a patent on the chips themselves and a copyright over the verification software so they would be the only company legally capable of

producing these chips. When another company, Tengen - Atari's NES development branch, tried to reverse engineer the chip Nintendo was able to successfully sue them for damages.

"HOMEBREW" GAMES

Ever since the Atari 2600, engineers have been attempting to crack machines for their own purposes. Items such as the "CuttleCart" enabled developers to create their own "homebrew" game making utilities. Flash Cartridges to which users could upload their own console ROM program was a cheap alternative for independent developers unable to afford the high price of licensed game console development kits. Aside from piracy, the cracking of Dreamcast's security spawned an incredibly large and diverse homebrew development community at http://www.dcemulation.com/. Aside from Sony's experiment with releasing a $700 development kit for the original Playstation called "Net Yaroze" (translated: "Lets Do It!"), this was a pretty big first in the console community. The other factor about the Dreamcast is that it had the ability to run a version of WindowsCE, which made porting applications from the Windows PC much easier. This ease of development wouldn't be matched until the leaking of Microsoft's XDK which made programming the Xbox as easy as booting up Visual Studio.

There is an interesting tug of war in the world of modded consoles. On the one hand, homebrew development is largely harmless, but on the other piracy can be incredibly devastating. While there is even evidence from a Microsoft software engineer that the Xbox mod scene influenced many of the capabilities of the Xbox 360 console (upon seeing the capabilities and ease of use delivered by a modded Xbox, Bill Gates himself was apparently quite impressed) - the numbers against piracy are hard for companies to ignore.

PC GAMES

The PC games industry is particularly hard hit. While pirating content on a console often requires a complicated process to get the machine to run unsigned/unauthorized code or bypass security checks, pirating PC games is largely just like pirating MP3s or movies - check out your favorite torrent site, download and apply the crack included with the torrent. Even long-time PC industry supporters like id Software - who originally started the entire trend of modding commercial PC games (which spawned not only very successful sales for their titles that supported modding, but launched countless careers of those developers who started via modding), have recently said that software piracy is truly reaching the mainstream. Recently expected blockbusters such as Call of Duty 4, Unreal Tournament 3, and Crysis have underwhelmed sales wise on PC. Instead more and more developers are looking to either abandon the PC market or at the very least begin supporting traditional game consoles.

This puts all the more pressure upon console manufacturers to make sure that their consoles are secure. While they might like to support or turn a blind eye to the generally legal homebrew applications, the impact of piracy demands more attention. For the past few years, companies like Sony have been incredibly aggressive at shutting down the manufacture and sale of modification hardware. There is a lot at risk when a for-profit pirate can modify a console, burn a bunch of games to cheap blank CDs and DVDs, and sell them to customers for a huge profit. Some extreme examples are businesses that keep a mirrored hard drive full of Xbox games and emulator ROMs and mass produce modded systems extremely efficiently.

While many gamers have huge respect for purchasing titles, not everybody does and the black market for games is quite large.

DRAWING THE LINE

On the other hand, there has also been a large amount of backlash over overly-intrusive protection schemes. One of the more aggressive protections - "StarForce" - installed rootkits onto user's computers and carried out activities such as "phoning home" to the publisher the user's behavior, reporting software applications installed to their computer, and broke compatibility with virtual CD drives. There was such a backlash over this technology that gamers actively boycotted the products or were actually encouraged to pirate the game because the pirated copy did not contain such protection.

Some publishers, such as Ubisoft, have chosen to abandon such aggressive measures in favor of less intrusive ones, but there is no kind of standard in the industry and other publishers continue to use varying degrees of protection which often just lead to more customer dissatisfaction. Many attempts to curve piracy completely backfire. Some developers even go the totally opposite route and abandon protection schemes altogether. A recently released title by StarDock called "Sins of a Solar Empire" was noted and renowned in the gaming community for not abusing honest customers but it is still yet to be seen if this is actually good or bad for their bottom line. As the video game industry has grown into a 20+ billion dollar worldwide market, there is an arms race to protect IP and copyright with no clear solution to the problem. Still, trying to tell a business executive they should do nothing about piracy would fly about as well as a led zeppelin.

TECHNICAL ELEMENTS

The technical details of physically modifying and installing chips onto the console hardware requires the person to be very familiar with electrical circuits and components and to old have the correct tools at hand, the first step of which is to void the warranty of the console system by opening its case. “Bunnie”, a famous Xbox hacker, mentions the lack of security in the hardware. “… console and secure PC manufacturers are not concerned about hardware security weaknesses, because hardware attacks are ‘too difficult for the average consumer to execute’”. This section will focus on some simple examples of reverse engineering and exposing vulnerabilities.

NINTENDO GAMEBOY

Because the GameBoy was in the market for handheld video gaming over fifteen years since its release in 1989, selling almost 120 million units (GameBoy and GameBoy Color) worldwide, it is very well-documented and due to its huge success, its flexible design philosophy has been used in several other consoles since. A simple look at the hardware specifications show a modified 8-bit Z80 processor with 8KB of internal RAM and 8KB of Video RAM, reading from cartridges of varying sizes from 32KB to 2MB.

During the Boot Sequence of the GameBoy, a 256-Byte program is executed from memory location $0 from an internal ROM, similar to a BIOS on a PC. This program computes and compares the cartridge’s checksum of the Nintendo logo, after which the internal ROM is disabled and the cartridge program is executed from location $100. All hardware registers along with the RAM are accessed as memory addresses between $0000 and $ffff, so one way some

GameBoy programs protected itself from piracy was through writing data into memory addresses such as the cartridge location itself, that the physical GameBoy would simply ignore but an emulator may interpret as valid.

The CPU opcode at cartridge address $100 is almost always a JP-address or a Jump-To-Address operation that directs the processor to the main chunk of the program. By overriding the Jump address, it is possible to redirect the GameBoy to boot and run other parts of code. And in the same way, if the program calls certain functions and Jumps to the code for that function, the address value can be re-directed to other functions, allowing inside gameplay to skip turns or damage calculation, and so forth. Cheating devices such as GameShark work this way by dynamically changing values of memory accessed by the GameBoy to create the desired behavior. Given the binary ROM file on a PC and a hexadecimal editor, the program could also be essentially re-written using this method as well.

MICROSOFT XBOX

All video game consoles have a boot sequence of some sort just as the GameBoy had in the previous section and the Xbox is no different. In the hardware initialization sequence, the Xbox has a backdoor flaw that allows the user to gain access to the boot-up RC-4 security key.

During initialization, the Xbox reads and interprets from a FLASH ROM in order to decrypt the compressed and encrypted kernel stored inside the FLASH ROM and place it in memory. As long as the kernel remains in main memory, other code can be run. Almost analagous to what was mentioned with the GameBoy boot sequence, by switching the data read from the FLASH ROM the user can gain control of the Xbox. The process works by starting

up the Xbox normally, then switching the contents of an unencrypted part of the FLASH ROM known as the jam table, and finally run a soft-boot (software-boot) which does not erase the main memory. By reading the contents of the main memory after the new jam table program is run, the Xbox kernel becomes exposed.

CAPABILITIES OF MODDED CONSOLES & SOFTWARE PACKAGES

There are many things that can be done with a modified, "modded", console. By bypassing the Digital Rights Management hardware and software built into the console, the user can put unofficial/unauthorized software packages onto the console that give you more control of the console's hardware.

XBOX MEDIA PLAYER

One of the most popular software packages available for the Xbox console is Xbox Media Center, the successor to the popular Xbox Media Player (XBMP) software. Some software packages require you to install an operating system such as Linux onto the Xbox to be able to execute; the Xbox Media Center, however, does not need an operating system. Instead, everything must be compiled into the XBMC executable via a custom, proprietary and non-free Xbox Software Development Kit, also known as "XDK". Not having a full operating system limits filenames in the XBMC to 42 characters. Also, the Xbox has four USB ports but the XDK does not contain a full USB-stack.

Aside from these minor problems that come from using unauthorized software, the Xbox Media Center transforms the Xbox console from a gaming console to a complete

multimedia center. With the XBMC, the Xbox can play most audio and video files and also can be used to launch programs such as emulators to play other consoles games on the Xbox console.

This allows the user to store all his media files and games to one place. Instead of having to sort through hundreds of DVDs, CDs, and game discs to find what you want, everything you need is located within the Xbox Media Center application. One big advantage that the Xbox Media Center has is the ability to stream files over a network, allowing users to store games and media files onto their Xbox but also the Xbox can play media files and games stored on the user's computer.

Because modded Xbox's have difficulties using the Microsoft Xbox Live service that unmodded Xbox consoles do not have, XBMC has added XLink Kai, a free alternative to Xbox Live. Whereby accidentally logging into Xbox Live with a hacked Xbox firmware, unlocked custom hard drive and boot dashboard will result in the console being permanently banned from the service, XLink Kai is a simulated worldwide Local Area Network that only consoles with the XLink Kai software can connect to. This service will not result in any kind of banning to your console. In addition to the online service, developers of XBMC have included features such as television program guides, YouTube, and Apple movie trailer support, as well as SHOUTcast/Podcast streaming, making the Xbox Media Center the best software package for a modded Xbox.

SOFTMODDING

We have already discussed how to modify a console's hardware to bypass the DRM, but there is a way to do this with software as well. This type of software is referred to as a softmod. Softmods usually exploit code used in the consoles save-game process. Once exploited, additional software can be added that will change the BIOS of the console. Once the BIOS are changed, new operating systems and new Xbox dashboards can be added to the console. This has made the process of modifying the Xbox extremely easy and fast. "With new technology and installers, softmodding has become an easy and reliable way to mod an Xbox. It is now considered an everyman's solution to a modded Xbox." (Wikipedia - Softmod)

Although there are many things that can be exploited using softmods, one of the most frequently used exploits is in the Xbox game Tom Clancy's: Splinter Cell. Using a security flaw in the save-game code in Splinter Cell, a user can load software onto the Xbox that makes it possible to install Linux onto the system. After Linux is loaded onto the Xbox, there are hundreds of different dashboards and applications that can be loaded onto the user's new Linux box. Or the console can even be used as a Linux server. This means people can buy cheap and easy to use Linux servers for their home or office. Once you have Linux on the Xbox, the system becomes a normal Personal Computer and can be used accordingly.

CONCLUSION / FUTURE OF CONSOLE SECURITY

In the end, while there are legitimate uses of modifying console hardware, they are largely overshadowed by the threat of piracy. Nintendo did not invest into any kind of protection for its Nintendo DS console and as a result it is possible to buy a cheap SD memory card, pair it with a specific $20 R4 compatibility card and load it up with ROMs off the Internet

for free. A standard 512MB card can usually hold around 15-20 games on it although the ability to manage the card with unlimited space on a computer makes any kind of limitation moot. Even though Nintendo has a hugely successful console, this still has a significant impact upon all the companies involved in making DS games. Nintendo is even one of the fortunate companies which actually make a profit off the cost of hardware. Sony and Microsoft use a loss-leader Gillette-styled strategy where the consoles are sold at a cost lower than it takes to produce them and they depend upon game sale royalties to overcome the investment to subsidize the consoles to a price people will buy them.

These companies are not resting on laurels however. All three of the console manufacturers have begun to brace the concept of networked consoles which brings forth a new paradigm in copy protection. While it is possible to log onto Xbox Live with a modded console, it is not an easy process and its extremely common for people to forget to enable the tricks that allow a user to go online undetected. For many people, the choice to mod your console will come with the inability to play games online with that console.

At the same time, services like Valve Software's STEAM, Microsoft's Xbox Live Arcade, and Sony's Playstation Network are embracing an age of digital distribution where the servers are able to verify a gamer's purchase and ability to play a game. Additionally, digital distribution is a solution to the problem of the used game market which many publishers claim to have a huge impact on their ability to make a profit. There's no copy to resell, and the digital version is signed to one user and one user alone. Prices are also much more controlled and traditional distribution costs are cut as well. It will be interesting to see how this is embraced in

the future. Currently, aside from STEAM and a few Playstation 3 titles, most of these digital titles are much smaller games than the kind typically sold in stores. Customers who are accepting of purchasing games typically priced in the $10 range at these online marketplaces may have a much different opinion when they are buying more ambitious games for the typical $50-60 retail price and being unable to ever resell them, trade them, or bring them to a friends house like one can with a disc.

All three console manufacturers are similarly embracing emulation. Sony emulates the original Playstation and Playstation 2 on the PS3, Microsoft the original Xbox on the 360, and Nintendo emulates a whole range of consoles on the Wii (NES, SNES, Genesis, Sega Master's System, Turbographix-16, Nintendo 64 and rising) under the guise of a "Virtual Console." What was once a big enemy is now being commercialized. Aside from online protection, Sony also has the advantage of a brand new media format with Blu-Ray. Blu-Ray disc burners are not mass-market like DVD and CD burners are, giving them some time to not only keep the Blu-Ray disc DRM from being cracked but keeping a large amount of people from having the capacity to burn disks. This will likely change over time but for now the format shift buys them time whereas both Microsoft and Nintendo have had their current consoles cracked for piracy.

At the same time as companies are embracing emulation technologies, both Sony and Microsoft have recently released PC compatible tools that allow homebrew and indie developers to create games with kits that enable compatibility with their respective console. Right now, they are still trying to figure out a way to possibly monetize this independent developer community so that they do not endanger their commercial developers but the

parallel between what factors have caused them grief in the past and what they are attempting to embrace is interesting. Sony is actually even more open with the PS3 allowing users to install Linux on the console and swap the hard drive out but still currently restrict access to proprietary graphics acceleration drivers owned by nVidia so the capabilities of Linux are still somewhat limited.

Clearly, the world of console copy protection is anything but clear-cut.

BIBLIOGRAPHY

"Bluehat07 @ Microsoft." 11 May 2007. bunnie's blog. 6 May 2008 <http://www.bunniestudios.com/wordpress/?p=171>.

Fayzullin, Marat. GameBoy Hardware. 6 May 2008 <http://fms.komkon.org/GameBoy/Tech/Hardware.html>.

Frohwein, Jeff. "Everything You Always Wanted To Know About GAMEBOY*." 17 March 1998. GameBoy Dev'rs - Docs. 6 May 2008 <http://www.devrs.com/gb/files/gbspec.txt>.

—. GameBoy Dev'rs - Docs. 13 September 2000. 6 May 2008 <http://www.devrs.com/gb/docs.php#faqs>.

Huang, Andrew "bunnie". Hacking the Xbox: An Introduction to Reverse Engineering. Stanford, CA: No Starch Press, Inc., 2003.

"id co-owner says piracy killing PC gaming." 7 August 2006. ArsTechnica. 4 May 2008 <http://arstechnica.com/news.ars/post/20060807-7440.html>.

"Is Bill Gates learning from the mod community?" 22 June 2006. ArsTechnica. 1 May 2008 <http://arstechnica.com/journals/thumbs.ars/2006/6/22/4415>.

"It's official: Ubisoft dumps StarForce." 14 April 2006. ArsTechnica. 4 May 2008 <http://arstechnica.com/news.ars/post/20060414-6603.html>.

"Nintendo 64 Emulator Writer RealityMan Calls it Quits." 8 March 1999. BNET. 6 May 2008 <http://findarticles.com/p/articles/mi_m0CGN/is_1999_March_8/ai_54047165>.

"Nintendo GC & Wii Security Flaws." 11 January 2007. Nintendo Wii Emulator. 6 May 2008 <http://wiiemulator.net/?p=4>.

"PC game developer has radical message: ignore the pirates." 20 March 2008. ArsTechnica. 4 May 2008 <http://arstechnica.com/news.ars/post/20080320-pc-game-developer-has-radical-message-ignore-the-pirates.html>.

"Piracy to blame for slowing PC game sales?" 17 January 2008. ArsTechnica. 4 May 2008 <http://arstechnica.com/journals/thumbs.ars/2008/01/17/pc-sales-slow-as-some-despair-over-piracy>.

"SoftModding the Xbox in 10 Minutes Using SID." 31 August 2005. XBOX-HQ.com. 6 May 2008 <http://www.xbox-hq.com/html/xbox-tutorials-183.html>.

The Cuttle Cart for the Atari 2600. 10 October 2003. 4 May 2008 <http://www.schells.com/cuttlecart.shtml>.

"THE FOX SPEAKS #3." 4 January 2004. EmuUnlim.com. 6 May 2008 <http://www.emuunlim.com/fox3.php>.

UltraHLE. 18 September 2000. 6 May 2008 <http://www.emuunlim.com/UltraHLE/>.

"Wii hacked it!" 30 January 2008. debugmo.de. 6 May 2008 <http://debugmo.de//?p=59>.

Wikipedia - 10NES. 2 May 2008. 5 May 2008 <http://en.wikipedia.org/wiki/10NES>.

Wikipedia - Console emulator. 2 May 2008. 6 May 2008 <http://en.wikipedia.org/wiki/Console_emulator>.

Wikipedia - Dreamcast. 5 May 2008. 6 May 2008 <http://en.wikipedia.org/wiki/Dreamcast>.

Wikipedia - Game Boy. 5 May 2008. 6 May 2008 <http://en.wikipedia.org/wiki/Game_Boy>.

Wikipedia - Net Yaroze. 1 May 2008. 3 May 2008 <http://en.wikipedia.org/wiki/Net_Yaroze>.

Wikipedia - Softmod. 13 April 2008. 6 May 2008 <http://en.wikipedia.org/wiki/Softmod>.

Wikipedia - UltraHLE. 29 March 2008. 6 May 2008 <http://en.wikipedia.org/wiki/UltraHLE>.

Wikipedia - XBMC. 26 April 2008. 6 May 2008 <http://en.wikipedia.org/wiki/Xbox_Media_Center#The_Video_Library>.

Wikipedia - Xbox. 6 May 2008. 6 May 2008 <http://en.wikipedia.org/wiki/Xbox>.