# Game Console Protection and Breaking It

**Nezer Jacob Zaidenberg**
*College of Management, Israel*

## INTRODUCTION

This chapter presents a survey of the attacks and defenses on various video game consoles (hereby consoles). Consoles are complex embedded systems designed to run various video games. At the console release time, the console is comparable to a high-end gaming PC. In addition to gaming hardware, the console also features an operating system and libraries. Unlike general-purpose PCs that run just about any software, consoles are supposed to run only licensed code and games. Consoles also include complex Digital Rights Management (DRM) and copy protection mechanisms. The attacks presented here are usually geared toward running custom OSs, homebrew (unlicensed) software and pirated games on the console. Over the last 20 years, various groups discovered the attacks against different consoles. Most of the attacks were reported by in the annual CCC conference.

The survey focuses on recent generations of game consoles (6th, 7th and 8th generation) as these are more interesting from a console hacking perspective. Prior console attacks usually used custom hardware modifications (modchips). These attacks are not comparable to attacks on newer generations, and therefore, older consoles are beyond the scope of this chapter. Also, this chapter does not deal with mobile consoles. (Such as PSP, Vita, Nintendo DS etc.) Last, Many other devices that can be considered gaming devices, particularly mobile phones (iPhone/Android). Also, PC-gaming is very common. (and PC games also suffer from piracy). These devices are not considered game consoles and are beyond the scope of this chapter.

## BACKGROUND

Consoles are a type of embedded system. Consoles offer processing capacities similar to a high-end PC.

However, unlike PCs, consoles hardware is geared entirely to run video games. At the time of release, consoles offer CPU, RAM, graphics capabilities and hard drive capacity comparable to a gaming PC. Furthermore, most consoles are cheaper than a comparable PC as the consoles' manufacturers subsidize consoles. The manufacturers sell the game consoles at a loss. Instead of profiting on console sales, the consoles' manufacturers profit when the users buy games.

Tools to attack the copy protection on consoles are as old as consoles themselves. However, the rising popularity of recent consoles has transferred the manufacturing modchips and tools to break the game console copyright protection is a flourishing business. As piracy is illegal, there are no official figures. However, the market size is significant. Console modchips cost roughly 50 USD apiece. Console sales often reach quantities of 40M to 100M units per model or even more in some cases. Most of these consoles are fitted with modchip at some point. These figures suggest that the modchip industry is a multibillion USD industry.

DOI: 10.4018/978-1-5225-9715-5.ch031

## Legality

It is off course illegal to pirate games. However, it is legal for the end-user to modify equipment that he (the end-user) owns. (fair use) Such modification can be, for example, installing modchips or software, provided the goal is not running pirated software but running homebrew code or Linux. It is also legal for the end-user to create backups of CDs that the end-user owns. (Playing backup CD is identical from a technology standpoint to playing a copied CD)

Installing modchips creates a loophole because, in the united states and other jurisdictions, thanks to the Digital Millenium Copyright Act (DMCA) it is also illegal to create devices whose sole purpose is to break DRM (such as modchips) even if no piracy is committed. So, in the united states, selling modchips designed to copy games is also illegal. Other countries have different laws and, in some jurisdictions, selling modchips may be legal. This chapter focus on the technology of attacks and defenses. The complicated international legal aspects of DMCA and game consoles are beyond the scope of this chapter.

Usually, modern console attacks no longer require modchips. However, it is worth noting that in 2011, Sony sued George Hotz (geohot) over DMCA violations regarding published PS3 attacks without using any modchip or hardware modifications.

The case was settled outside court, and Hotz committed not to hack another Sony product.

However, even software only attacks (i.e. running code that the user has coded on an embedded device that the user own) may result in legal action, in the USA.

## Motivation

The obvious motivation beyond attacks on game consoles is piracy. Console games are expensive. Console games are even more expensive than PC games. The PC version of the same game is usually cheaper than the console version due to royalties e collected by the console manufacturer to cover the subsidized cost of the console itself.

However, in addition to piracy, there are several other motivations behind attacking game consoles. The first of those is running other operating systems, usually Linux. As game consoles offer high-end (for the release time) hardware at subsidized costs using game consoles as regular computers and running Linux has appealed to hackers. Furthermore, according to DMCA, it is considered legal and fair use of the end-user equipment. The console manufacturer attempts to prevent running Linux as console games will not be purchased for Linux server. Since the console itself is subsidized the manufacturer loses money if the end-user installs Linux on the console.

Another potential motivation is running homebrew software, i.e. software that the user coded (or open-source software the user compiled) on its own machine. This use case is also legal, according to DMCA. I.e. it is considered fair use.

There are two risks from the console manufacturer point of view with running homebrew code.

The first is unlicensed games. The console manufacturer is subsidizing the console sales but collecting royalties from any game sold. This is possible only because the manufacturer has complete control (using signatures) on what is allowed to run (whitelisted, signed) to run on the machine. Unlicensed games don't allow the manufacturer to collect royalties. Therefore, unlicensed games without paying royalties should not be allowed to execute on the machine.

The second problem with homebrew code is that it removes the manufacturer control over the entertainment system at the end-user's digital home. Console manufacturers frequently have additional goals in this field (enforcing standards, formats, operating systems to use etc.) Therefore, The console users

## Related Content