Interactive entertainment has developed into a multibillion dollar industry over the past 50 years. For much of that period developers of games have been embroiled in a costly arms race against software piracy that has resulted in untold billions of dollars of lost revenue. Whether on the PC or on home consoles, software pirates have devised ingenious schemes to circumvent digital rights management (DRM) nearly as quickly as DRM has been devised. Given that DRM is a practical security problem with a long history, we hope to draw out some interesting observations and lessons about best practices where a real-world security challenge meets a real-world industry.

We will discuss and draw lessons from a variety of tested and failed DRM schemes, from charmingly primitive early attempts to the far more sophisticated fare of the last 10-15 years. Finally, of particular note to us will be the current reigning security scheme on the PC, a proprietary software protection suite called Denuvo that has proved conspicuously durable against attackers since its introduction in late 2014.

An infamous early DRM scheme used in the 1980s and early 1990s leveraged the assumption that legitimate owners of a game would possess a physical copy of the title including a user’s manual; the software would then ask the player for some information only obtainable in the manual (i.e. what is word 12 on line 15 of page 25?) as a means of copy protection. Obviously this scheme was not durable in the advent of the internet age, and lives on now as a significant annoyance if one wants to go back and play games from this era.

In the home console area, much can be made of the business ramifications of decisions motivated by software piracy concerns. Fearing the ease of piracy of up-and-coming CD technology, Nintendo opted for a proprietary cartridge-based software delivery system with 1996’s Nintendo 64, a factor which contributed to increased end-user cost and limited storage space, both of which helped open a path for Sony to enter the market as a legitimate competitor. The very rudimentary security scheme of 1999’s Sega Dreamcast made pirating software not much more difficult than burning an ISO to a CD, a factor which contributed to the failure of the Dreamcast and the complete exit of Sega from the hardware market. In the modern day, a massive security exploit in Nintendo’s current handheld console, the Nintendo 3DS, has made it possible to crack any console with any firmware to download and play the console’s entire library- directly from Nintendo’s own servers! This has hastened Nintendo’s move to their next generation console, the Nintendo Switch.

Beginning with CD-key protection schemes similar to those used in other commercial software, modern PC security schemes have experimented with a variety of approaches. These include obtrusive software designed to prohibit tampering with the game executable, such as SecuROM and Punkbuster, schemes which were so obtrusive they were infamous for appearing as viruses to antivirus software due to tampering with the system at an OS level. Other schemes have involved periodic online activation and reactivation of the product, guaranteeing a maximum number of installs across all systems per product license. Other titles have opted to require users to be online, and in constant communication with a game server, in order to use the title. Common to many of these schemes is some amount of frustration and inconvenience for even legitimate end-users.

Denuvo was first implemented in a PC game in 2014. It is a proprietary protection suite licensed to game developers by Denuvo Software Solutions GmbH out of Austria. Since its inception it has become the de rigeur protection scheme for many PC titles. Denuvo is notable for its high degree of success over a prolonged period in a fast-moving field with a long history of failures. Being a proprietary scheme, and one undergoing continuous undisclosed development and refinement, we can only hazard our best guesses about implementation details. What is clear is that developers must work with Denuvo on integration of the protection scheme with the game executable; when this is done improperly the scheme can be surmounted just as easily as in the bad old days, as happened within days of the release of January’s Resident Evil 7.

To briefly comment on a radically different approach to the DRM problem, we note the continued success of the digital storefront GOG, short for Good Old Games. GOG’s main point of differentiation from competitors like Valve’s Steam or EA’s Origin is that it sells games with no DRM whatsoever, which can easily be copied, backed up, and distributed maliciously. Yet the success of GOG, and the continued willingness of many PC developers to sell games on GOG’s platform, presents the possibility that end-user weariness with obtrusive protection schemes has become a significant factor driving PC purchases.

In conclusion, DRM in entertainment software is a continuously developing area where one can see the challenges that security schemes face against real-world attackers in vivid, blow-by-blow detail. Particularly, what comes out of the study of the problem is the sense in which real-world security schemes are a reaction to forces of the market, and often a cause of such forces as well.