The Hyper Visor

In my teen years getting through Microsoft hypervisor patches was my fun. Exploiting hypervisor hashes and bypass their authentication system was a gold mine to exploit teens that were fare less knowledgeable in this field that I am.

It all began back in the 8th grade. Hypervisor exploitations were something that was just beginning. Kids would buy broken Xbox’s off of eBay, extract the key vault off of it and sell it online to kids for 70 dollars a pop, an easy 50$ profit. For the reader who doesn’t know what a key vault is, it is a special file on the console that allows it to access the Internet. When Microsoft sees that you have a modified console they will ban the key vault so that the console cannot access the internet anymore and you are not able to run restricted code that can alter the game state. Each update the hypervisor changes, thus causing the keyvault to change its code. Meaning that you need to reverse engineer the hypervisor to decrypt the key vault and in turn allow it to run on the console successfully. This is where I would come in. PPC is a language that allows the reverse engineering of the hypervisor that will allow the keyvault to run on the console. The part that I find interesting and how it relates to security is the ability for an amateur teen with access to the console PCB, a computer, the hypervisor, and the web I am able to reverse engineer the hypervisor to allow the console to run restricted code that is normally not allowed. This is a prime example of Microsoft’s failure to patch the access of the hypervisor by leaving vitally prone access points on the physical console itself vulnerable to curious teens, like me, waiting to exploit them with the power of copper wire and a soldering iron.

Physical. On the physical Xbox PCB board itself lies certain pins that if soldered correctly together and linked to the serial port on your PC can allow you to access your NAND which in then turn allows you to access the Hypervisor using a nifty program called Xe-Build. Microsoft has failed, since the original Xbox 360 release in 2006, to properly patch access to these pins and thus allowing people like me to exploit them maliciously. This could be an extremely simple fix, either by hiding these pins or covering them up with other crap such as useless heat sinks or shrouds that don’t make it obvious.

Software. With 3 weeks, I was able to learn PPC. Reverse engineering the hypervisor was a breeze after 3 others and myself spent 3 weeks decoding and reversing the hashed hypervisor back to its original state so we can locate the correct memory location where the key vault is stored thus allowing us to extract it and either sell it or use it ourselves to run code on our consoles maliciously. After learning about encryption in school, and all the various tactics that computer scientists use to hash their code and encrypt their files, a simple hand shake method with Microsoft servers and the console to run a code to verify that the console is in fact running its OWN key vault and not a key vault that was extracted off of another console is an extremely simple way to combat this. Too bad, they will never implement it.

Security? Microsoft has struggled with security for years. Not as much as Sony, however they have struggled with security breaches through the Xbox live system spanning back to the release of the original Xbox. Do they not care? Or is it a simple act that it is not worth their time to create a system to combat this. Even with their patrol system’s that monitor user usage and fair gameplay, it still takes up to 36 hours to ban a console that is running unauthorized code.

Lesson? Microsoft needs to get their shit together. Hire someone who has already played and been through the system. Let that person fix your issue. If you want to stop mischievous teens like me from breaching your system and altering the game state of players who are trying to enjoy the game, hire me. I will fix your problem, however they don’t care, and people like me will continue to make the game unfair for other kids who try to play. GG. ☺