Sony and Rootkits: Digital Rights Mismanagement

Joe Kardamis

The news of Sony's invasive Digital Rights Management (DRM) scheme hit the internet on October 31, 2005, on the weblog of Mark Russinovich of Sysinternals [4]. After running a scan for rootkits, he was surprised to find one on his machine. He was further surprised and angered that it came at the hands of a Sony music CD, which had installed a series of drivers which were hooking, among other things, the CD player drivers to keep track of what was being played and or copied, as well cloaking directories and the registry. Such a technique was not only extraordinarily unethical, as there was no mention of such behavior in the EULA [5], and of dubious legality (several class-action lawsuits were filed, the first of which coming from California [3]), but it was also sloppily created. Beyond the obvious security risks posed by such a rootkit (the compromise of one's machine), this set of programs left the system wide open to further exploitation from other malicious attackers, as well as threatened the reliability and operability of the machine. I will detail what these further risks were, and examine the reactions of various involved people and companies, including leading security experts, the company hired to write the software, and Sony itself. This story is a major example of why understanding computer security is so important, and also of the state of affairs in computing and audio entertainment.

As detailed by Russinovich, Sony's DRM software took control over aspects of the customers' now infected computers, leaving them vulnerable in ways in which neither Sony nor First 4 Internet (the company hired to write the invasive software) expected. The software was designed not to be detected, and to enforce a three-copy limit of the music CD, also ensuring that the copies would not be usable to create more copies. To achieve the necessary stealth, the rootkit hides all files and directories prefixed with a particular string: "sys". This is a rudimentary form of file hiding, which is in and of itself insecure. While it performs the intended job, it also allows others to exploit this weakness by hiding other files on the infected machine prefixed with the magic string. And in fact it did not take long for instances of such exploits to show up in the wild. One such instance used this exploit to cheat the anti-cheating program in the popular MMORPG World of Warcraft. By using the magic string as a prefix, the anti-cheating program could not detect the offending scripts [1].

If a user did manage to detect the presence of Sony's rootkit, in attempting to remove it, they would likely render their CD drive, if not their entire machine, useless. Another included driver in the rootkit nested itself in the driver chain attached to the CD drive. By removing the driver, the chain to access the hardware is broken, and thus the drive is made inaccessible. Once this was all brought to light and Sony was forced to provide a means for removal (which is another issue in and of itself; more on that later), the method used to purge the machine of the drivers was in and of itself unreliable. The way in which the driver was uninstalled was identical to simply stopping the service (net stop). However, because the rootkit deals with hooked function calls, in a multi-threaded environment there is the potential for the functions to be improperly referenced, resulting in a Blue Screen of Death [4].

The reactions of security expert Mark Russinovich ranged from irritation, incredulity, and sheer anger. These were directed both at the fact that users were unknowingly agreeing to infecting themselves with dangerous software, which was mentioned nowhere in the EULA, that the software was so poorly constructed, and at the responses of Sony and First 4 Internet. In his blog, Russinovich details the behavior of the rootkit, as well as the issues involved with its removal [4]. Not only does the kit hide files and alter the registry, but it also contacts Sony with information regarding the CD being played. This was ostensibly done so new and updated content could be served to the user, and was deemed as one-way communication by First 4 Internet [6]. Such "phone home" behavior was flatly denied by Sony. The latter was proven false by Russinovich, who used a network tracer to find the packets being sent to Sony by the rootkit, which had encrypted with it the CD's identification. The former was argued as nonsensical, as, while Sony was probably not actively making use of the data in reprehensible ways, they certainly had the facility to. The idea of "one-way" internet communication is farcical in and of itself. Additionally, Sony required that, should a user want to remove the software from their machine, they were forced through such hoops that Russinovich compared some adware companies' methods of product removal more favorably than Sony [7].

First 4 Internet, among attempting to argue that the communication between the rootkit and Sony was "one-way," also attempted to refute Russinovich's allegations of incompetence. They dismissed his diagnosis of their unsafe unloading of the driver as "pure conjecture." This "conjecture" is however, part of nearly every textbook example of multi-threaded race conditions, and while it may be unlikely, it is certainly not conjecture.

Bruce Schneier weighed in on the issue as well, and laid some blame to the security companies such as McAfee and Symantec. These companies were extraordinarily slow to provide the facilities to detect and neutralize these threats, when for most other pieces of malware they are quick to respond. Given that the propagation of the rootkit resulted in over one half million compromised machines, the companies designated to protect the user from such malicious software dropped the ball in a large way. And when they did respond, their proffered solutions were no better than those provided by Sony; an unsafe halting of the service which could result in a system crash. While Schneier does not blatantly accuse the security companies of collusion or other underhanded behavior, he paints a grim picture of "what ifs" having the same affect [9].

Sony, as the main perpetrator, both flatly denied any amount of wrongdoing and displayed an inordinate amount of arrogance. They lied by omission in the End User Licensing Agreement, by not disclosing to users what the software truly did, they lied in their refutation of the software contacting them, and they made it extraordinarily difficult to obtain the mechanisms to remove the software. Thomas Hesse, the president of Sony BMG's global digital business was so brash as to say "Most people don't know what a rootkit is, so why should they care about it?" in an interview with NPR [2]. Such a unified negative corporate response could be indicative of gross negligence, gross incompetence, or gross malice. Likely it is a combination of the three, but even so, it is unsettling. It is truly indicative of the lengths that these corporations will go to protect their bottom line. Digital Rights Management is a hotly contested topic, and in Sony's eyes, they are merely attempting to prevent theft. However, the way in which they attempted to solve the problem was extraordinarily irresponsible. There is no simple and easy solution to the DRM problem, and it seems likely that the rootkit issue as applied to DRM will not yet go away. In official statements, Sony stated that it was temporarily halting production of CDs containing the offending software [8]. The unnerving term being "temporarily," which seems to suggest that once the backlash has settled, they may try again. Sony has since made the appropriate information regarding the insecure nature of their software public on their website, and the uninstaller has been made public as well [10].

I fear that things are going to get worse before they get better, although the topic has been relatively quiet compared to when the news first broke almost a year ago. As digital media progresses, and the ability to quickly and accurately copy and distribute such media continues, theft will continue to be an issue, and I feel that the media companies will continue attempting invasive measures to secure their bottom line. It is extraordinarily easy to cast blame and condemn Sony's actions as morally and legally wrong, but it is altogether more difficult to come up with better alternative solutions. And I am not innocent, for I clearly think Sony was completely in the wrong, but I have no alternate solution to offer. Until that alternate solution is found, if one is found at all, I fear that we as users and consumers will be made to endure further failed and invasive attempts at corporations trying to protect their privacy at the expense of our own.

[1] Register, The. (2005, November 5). *World of Warcraft hackers using Sony BMG rootkit*. Retrieved October 22, 2006, from http://www.theregister.co.uk/2005/11/04/secfocus_wow_bot/

[2] Roberts, Paul F. (2005, November 8). *Sony's Second 'Rootkit' DRM Patch Doesn't Hush Critics*. Retrieved October 22, 2006, from http://www.eweek.com/article2/0,1895,1883820,00.asp

[3] Roberts, Paul F. (2005, November 11). *Sony Suspends 'Rootkit' DRM Technology*. Retrieved October 22, 2006, from http://www.eweek.com/article2/0,1895,1885868,00.asp

[4] Russinovich, Mark. (2005, October 31). *Sony, Rootkits, and Digital Rights Management Gone Too Far*. Retrieved October 22, 2006, from http://www.sysinternals.com/blog/2005/10/sony-rootkits-and-digital-rights.html

[5] Russinovich, Mark. (2005, November 4). *More on Sony: Dangerous Decloaking Patch, EULAs and Phoning Home*. Retrieved October 22, 2006, from http://www.sysinternals.com/blog/2005/11/more-on-sony-dangerous-decloaking.html

[6] Russinovich, Mark. (2005, November 6). *Sony's Rootkit: First 4 Internet Responds*. Retrieved October 22, 2006, from http://www.sysinternals.com/blog/2005/11/sonys-rootkit-first-4-internet.html

[7] Russinovich, Mark. (2005, November 9). *Sony: You don't reeeeaaaally want to uninstall, do you?*. Retrieved October 22, 2006, from http://www.sysinternals.com/blog/2005/11/sony-you-dont-reeeeaaaally-want-to_09.html

[8] Russinovich, Mark. (2005, November 14). *Sony: No More Rootkit - For Now*. Retrieved October 22, 2006, from http://www.sysinternals.com/blog/2005/11/sony-no-more-rootkit-for-now.html

[9] Schneier, Bruce. (2005, November 17). *Sony's DRM Rootkit: The Real Story*. Retrieved October 22, 2006, from http://www.schneier.com/blog/archives/2005/11/sonys_drm_rootk.html

[10] Sony BMG. *Information about XCP Protected CDs*. Retrieved October 23, 2006, from http://cp.sonybmg.com/xcp/english/updates.html