Ethical issues surrounding the sony rootkit

Extended Copy Protection (XCP) is a software package developed by the British company First 4 Internet (F4I) and sold as a copy protection or digital rights management (DRM) scheme for compact discs (Wikipedia 2005).

This software is designed to control the distribution (copying) of material on compact discs. One version of this software, ‘ XCP-Aurora’, was used as a copy protection measure by Sony in 2005. This software was discretely included in many Sony music CD’s at that time. On the first occasion that a user attempted to play or copy music from a CD containing XCP, the software was automatically installed on the users system. It is noteworthy that this only applies to the Microsoft windows operating system; the software had no effect when used in conventional CD players or on computers running Linux or other operating systems.

The key ethical point at this time is that this software was installed entirely without user knowledge or consent. Furthermore there was no way to safely remove the software from an affected CD, in fact some attempts could result in rendering CD drives inoperable due to registry settings adapted by the software on installation. The fact that the software was designed to be hidden and installed without consent has led to it widely being described as Spyware (the term Rootkit is used for reasons I will describe later). In order to examine the ethics of this situation I believe that first one needs to examine why Sony used this software in the first place.

In the past Sony have enjoyed a very generous share of the entertainment market. As new technologies have been developed and made available, this share has diminished. In particular Web based companies such as napster or

Itunes have been created in direct opposition to Sony who sell their entertainment on CDs/DVDs. As this rivalry developed Sony adopted an aggressive stance.

“ The industry will take whatever steps it needs to protect itself and protect its revenue streams... It will not lose that revenue stream, no matter what...

Sony is going to take aggressive steps to stop this. We will develop technology that transcends the individual user. We will firewall Napster at source – we will block it at your cable company, we will block it at your phone company, we will block it at your [ISP]. We will firewall it at your PC.

.. These strategies are being aggressively pursued because there is simply too much at stake. ” (Sony Pictures Entertainment US senior VP Steve Heckler, August 2000).

This quote was in fairness taken at a time when napster was simply allowing users to download music at will and without charge but it does provide an insight into the company mentality of Sony with regard to internet based competition. Sony’s public reasons for including the XCP-Aurora software was that the software was to protect CD’s from unauthorized copying and ripping. A rootkit is defined as a set of software tools frequently used by a third party (usually an intruder) after gaining access to a computer system. These tools are intended to conceal running processes, files or system data, which helps an intruder maintain access to a system without the user’s knowledge (Suzi Turner ZDnet.

com Blog Nov 18 2005). One of the main operations of the XCP-Aurora software is to conceal its own existence. It does this in the manner of a rootkit, leading to its more common name, The Sony Rootkit. The international community however took a very different stance on the use of the software however.

The general response being that Sony had gone too far in protecting its own commercial interests. The software package installed intercepted any media playing or ripping software other than the package included on the disc forcing users to use Sony’s own software to access the media files on the discs. While this package allowed the user to play the songs on the CDs, it limited the number of times that the music could be copied to other CDs or to portable devices such as MP3 players. Furthermore only supported portable devices could be used. Particularly the popular Ipod mp3 player, produced by Sony rival Apple was not supported. This therefore prevented owners of an Ipod from playing the music they had legally purchased on their portable device.

This is a major feature in the ethical debate. Did Sony have the right to prevent users from playing their music in a manner that they choose? Keeping in mind that this is not a piracy or a distribution issue, this affects a user who wants to listen to music tracks they have purchased on their own portable device. The Apple Ipod is a very popular, widely distributed device. Sony cannot claim ignorance to the fact that a large number of individuals that purchase their CDs would also own an Ipod and would rightly wish to play the music using this device. The exclusion of the Ipod from supported products is very spiteful and shows a complete disregard for the interests of

their customers. The Sony brand is well recognized and trusted worldwide and as such they have an ethical responsibility to justify that trust, instead they have abused it.

Even the design of the Rootkit Software was ill conceived. The software was intended to hide from the user as I have already discussed. The manner in which this goal was achieved however was, at the very least, careless. The method of camouflage used was to hide any system process with a name with a prefix sys. Obviously Sony ensured that all the processes their software would run had this prefix. However there was a very noticeable and one would have thought obvious side affect to this.

It meant that the software was not exclusively hiding its own functions; any process with this prefix would be hidden. This provided hackers and virus producers with a very potent back door opportunity. Within weeks of the software’s release onto the market there were a number of worms and Trojans exploiting the security holes caused by Sony’s software. It is also noteworthy that the installed software runs constantly, not only when a CD is being used or music played/copied. This meant that system resources were being used at all times, potentially slowing down affected computers while leaving no way for the user to stop the running processes. The software’s discovery stemmed from a number of system crash reports to Microsoft relating to the file aries.

sys; however this file could not initially be found on any affected systems. It has later been shown that this file is part of the XCP Aurora software. There were also an increased number of ‘ missing’ drives, a symptom of a failed

attempt to remove the software manually. Its discovery led to a very fast growing scandal for Sony. They responded with a measure to stop the ‘ piggybacking’ of hackers.

Sony also contends that the “ component is not malicious and does not compromise security,” but “ to alleviate any concerns that users may have about the program posing potential security vulnerabilities, this update has been released to enable users to remove [the root kit] component from their computers. ” (Thomas Hesse, President of Sony BMG’s global digital business division, 2005). However no uninstaller program was provided so users were still faced with very limited use of the product. A settlement was however reached at a hearing on May 22nd 2006.

In short the settlement (1) forbade Sony from producing discs containing XCP software (2) demanded that they provide updates fixing all known security vulnerabilities that the software caused and (3) demanded the provision of software to safely remove the XCP-Aurora software from affected PCs. There were also reparations for affected users in the form of replacement CDs lacking in XCP software or free album downloads. One could be forgiven for thinking that things couldn’t have gotten much worse for Sony at this stage but in fact the initial software provided to users to uninstall the XCP software carried with it its own security vulnerabilities. Security researchers quickly discovered that this removal toll contained an insecure ActiveX control.

This security glitch could allow arbitrary code to be installed on an affected system, although the user would have to visit a malicious website (Secunia. com). Once this flaw became apparent Sony stopped distribution of the tool

but this was little comfort for users that had already used it. Taking all of the evidence into account, it is fair to say that Sony took a very selfish and short-sighted approach to dealing with an industry which is expanding at an accelerated rate.

Advances in technology were producing new kinds of rivals in the market and instead of adapting their own products to make themselves more competitive, Sony opted for a more attack minded approach. However in doing this they either failed to consider the effect it would have on their customers or they decided that it was a risk worth taking. Whichever of these options is more accurate, it is unacceptable behaviour for a company of Sony’s standing. The Sony brand is recognized worldwide and consumers are inclined to trust that if they buy a Sony product they are obtaining a certain level of quality. In short this trust was abused.

After all the initial embarrassment of the scandal Sony should have taken some time to reflect on the whole issue. Instead they rushed into making promises and producing quick fix tools which, as I have already mentioned caused their own security risk that many considered to be a greater security threat than the original rootkit. As I have mentioned already Sony maintain that the purpose behind the software was purely for copy protection. If this was truly the case then I think that people would accept that while mistakes were made in its application, they were perhaps ‘ honest’ mistakes. However when considering all the facts, and looking in particular at the fact that the Apple Ipod, one of the most common portable music devices in the world, was blocked by the program it is clear that copy protection was not at the forefront of Sony’s thinking.

Their primary concern was their own financial interests, mainly related to competition. What they underestimated or failed to predict was the mass of negative publicity that came from the scandal. In the end the whole affair was a public relations nightmare for the company and it will be a long time before the international community forgives or forgets the incident. If the goal was indeed to gain an advantage over the opposition then I think that precisely the opposite effect has been achieved. Bibliography and References 1) Suzi Turner, ZDNet.

com Blog: Rootkits galore: part I http://blogs. zdnet. com/Spyware/? p= 706 2)www. ikipedia.

com : http://en. wikipedia. org/wiki/Sony_rootkithttp://en. wikipedia.

org/wiki/2005_Sony_BMG_CD_copy_protection_scandal 3) SONY BMG Music Entertainment http://cp. sonybmg. com/xcp/ http://www. sonybmgcdtechsettlement. com/ 4)The Register http://www.

theregister. co. uk/ http://www. theregister. co.

uk/2006/05/23/sony_rootkit_settlement/ http://www. theregister. co. uk/2005/11/17/sony_drm_uninstaller_peril/ http://www. theregister.

co. uk/2005/12/29/sony_settles_rootkit/ 5)www. Secunia. com http://secunia. com/advisories/17610