Electronic Frontiers Australia
Supplemental Submission to the House Standing Committee on Legal and Constitutional Affairs Inquiry into Technological Protection Measures Exceptions

Introduction

Electronic Frontiers Australia ("EFA") thanks the Committee for the opportunity to make this supplemental submission, which will address several issues which have arisen since the making of our first submission.

Sony's "rootkit" Technological Protection Measure

On 31 October 2005, a software developer published a report that he had discovered the existence of a "rootkit" on one of his computers, and that further investigations had revealed that the rootkit had been installed by the Technological Protection Measure (TPM) embedded in an audio CD released by Sony BMG.[1]

A "rootkit" is a software tool, or set of tools, which are designed to conceal the presence and operation of other (typically malicious) software from users of a computer, even those possessing some degree of technical skill. Rootkits have traditionally been used by computer "hackers" to cover their tracks and avoid detection.

The rootkit used by the Sony TPM acts as a type of "cloaking shield", preventing Microsoft Windows from displaying any file, directory, Registry key, or running program whose name begins with the pattern "$sys$". Users with this TPM installed on their computers would be unable to see the files comprising the TPM, or detect that the TPM was running on their computer.[2]

An unintended consequence of this is that *any* file whose name begins with "$sys$" will be hidden from Windows – not just the TPM components. This represents a major security risk, and there are already viruses which exploit this behaviour to hide themselves inside infected computers.[3]

Other components of the TPM are misleadingly described as "Plug and Play Device Manager"[4] or "network control manager"[5] in an attempt to deceive users

[1] Mark Russinovich, *Sony, Rootkits and Digital Rights Management Gone Too Far* (2005) Mark's Sysinternals Blog <http://www.sysinternals.com/blog/2005/10/sony-rootkits-and-digital-rights.html> at 22 November 2005.

[2] Ibid.

[3] *First Sony BMG 'Rootkit' Virus Reported* (2005) FOXNews.com <http://www.foxnews.com/story/0,2933,175188,00.html> at 6 December 2005; *First Trojan using Sony DRM spotted* (2005) The Register < http://www.theregister.co.uk/2005/11/10/sony_drm_trojan/> at 6 December 2005.

[4] Ibid.

[5] Mark Russinovich, *More on Sony: Dangerous Decloaking Patch, EULAs and Phoning Home* (2005) Mark's Sysinternals Blog <http://www.sysinternals.com/blog/2005/11/more-on-sony-

who discovered them into believing that they were a harmless part of Microsoft Windows.

The TPM and its associated rootkit do not appear in the Windows "Add/Remove Programs" facility, nor is there any other way given to uninstall them. Simply deleting the "cloaked" files in an attempt to remove the TPM results in the computer's CD drive no longer working.

The behaviour of this TPM is objectionable for several reasons, including that:

1. The End User License Agreement (EULA) for the TPM software makes no mention of rootkits, or that the TPM software acts invisibly to the user of the computer;
2. The EULA does not disclose that the TPM software being installed cannot be uninstalled;
3. The EULA does not disclose that attempts to remove the TPM software by deleting it will disable the computer's CD drive;
4. The rootkit installed by the TPM presents a security risk in that it enables any other software to hide itself, including viruses and other types of malicious software;
5. The installation of the rootkit in these circumstances may constitute a breach of criminal law; and
6. The EULA does not disclose that the TPM software acts as spyware, transmitting information to Sony BMG about what discs are being played.

Sony's actions in distributing this TPM have been widely condemned. Sony's response has been to deny any wrongdoing, stating that "Most people don't even know what a rootkit is, so why should they care about it?"[6]

Sony has been sued by the state of Texas, alleging breaches of that state's anti-spyware laws, and also sued in a class action by the Electronic Frontier Foundation.[7] A separate criminal complaint is under investigation by Italian authorities.[8]

dangerous-decloaking.html> at 6 December 2005.

[6] Neda Ulaby, *Sony Music CDs Under Fire from Privacy Advocates* (2005) National Public Radio <http://www.npr.org/templates/story/story.php?storyId=4989260> at 6 December 2005.

[7] *Texas, EFF sue Sony over 'spyware'* (2005) Sydney Morning Herald <http://www.smh.com.au/news/breaking/texas-eff-sue-sony-over-spyware/2005/11/22/1132421627766.html> at 6 December 2005.

[8] *Italian police asked to probe Sony copy protection code* (2005) Computerworld <http://www.computerworld.com/securitytopics/security/story/0,10801,106064,00.html?source=NLT_PM&nid=106064> at 6 December 2005.

In an ironic twist of fate, it has been alleged that the Sony TPM software incorporates software code from open-source projects, in violation of the applicable open-source software licenses. That is, the Sony TPM software itself is said to infringe copyright – or to use the terminology more favoured by entertainment industry groups, Sony has "stolen" copyright material and are illegally distributing it for commercial gain.[9]

EFA submits that Sony's actions are arguably illegal under Australian law for several reasons, including:

1. That Sony has engaged in misleading and deceptive conduct within the meaning of s 52 of the *Trade Practices Act 1974*;
2. That the Sony TPM installing a rootkit without the computer user's consent constitutes a tortious trespass to chattels;
3. That the Sony TPM installing a rootkit without the computer user's consent may be a criminal offence under Commonwealth and State laws applying to fraud, and computer "hacking" and misuse;[10] and
4. That the Sony TPM infringes copyright by including code obtained from open-source software projects in breach of the applicable license.

Yet, even if Sony and their TPM software are in breach of Australian law, under the FTA, their TPM would still enjoy anti-circumvention protection. It would be illegal for consumers to circumvent the TPM to play protected CDs without installing the TPM software (and the rootkit). It may be illegal for consumers to uninstall the TPM from their computers. Tools which would facilitate the bypassing or removal of the TPM would be "circumvention devices" and criminal sanctions would apply to dealings with them.

EFA submits that it is manifestly contrary to public policy that anti-circumvention protections extend to TPMs which operate or are distributed in ways which breach Australian law.

EFA further submits that an exception to the anti-circumvention provisions of the FTA is required to ensure that such TPMs may be lawfully circumvented.

[9] *Spyware Sony seems to breach copyright* (2005) De Winter Information Solutions <http://dewinter.com/modules.php?name=News&file=article&sid=215> at 8 December 2005.

[10] E.g. *Criminal Code 1899* (Qld) s 408D.

Construction of the relevant FTA provisions

EFA wishes to endorse the recommendations contained in Part 3.2 of the submission of Kimberlee Weatherall, on the proper construction of relevant sections of the FTA.

The DMCA rulemaking process

Numerous submissions made by groups representing the interests of copyright holders have referred favourably to the "rulemaking process" used in the United States to create exceptions to the anti-circumvention provisions of the Digital Millennium Copyright Act.[11]

EFA has grave concerns about the fairness, complexity, and accessibility of this rulemaking process, and the standards of proof required under it. EFA submits that the result (if not the intent) of this process is to make it prohibitively difficult to gain new exceptions, especially for end-users of technology who cannot afford or obtain legal assistance.

We refer the Committee to a recent report[12] prepared by the Electronic Frontier Foundation, which is Exhibit 1 to this supplemental submission. EFA strongly endorses this report and it's recommendations, and believe that it will provide the Committee members with a valuable perspective on the US rulemaking process.

(The Electronic Frontier Foundation is not in any way associated with EFA. EFA is completely independent of EFF, and is not and has never been an affiliate, subsidiary, or "branch office" of EFF.)

EFA again wishes to thank the Committee for the opportunity to make this supplemental submission.

Sincerely,

Dale Clapperton
Vice-Chair and Convenor of the Intellectual Property Committee
Electronic Frontiers Australia

[11] eg International Intellectual Property Alliance submission at p 4-7; Australian Federation Against Copyright Theft submission at p 8-10; Business Software Association of Australia submission at p 3-4; Interactive Entertainment Association of Australia submission at p 7-13

[12] *DMCA Triennial Rulemaking: Failing the Digital Consumer* (2005) Electronic Frontier Foundation <http://www.eff.org/IP/DMCA/copyrightoffice/DMCA_rulemaking_broken.pdf> at 8 December 2005.