Proposal for Discussion by EURIM and others

Authors:
Michael Barwise, Consultant, Computer Security Awareness
mike@computersecurityawareness.com

Niels Bjergstrom, Editor-in-Chief, Information Security Bulletin
Senior Consultant, Computer Security Engineers Ltd
njb@chi-publishing.com

Stuart Ritchie, Consultant
stuartritchie@radsql.com

Hacker's Charter? Legislative Enshrinement of Software Insecurity

"The bad guys aren't going to publish the results [of security analyses], they're just going to exploit them... We should be eliminating the laws that encourage insecurity."

Barbara Simons, referring to the ACM's proposed amendment to DMCA[1]

Proposal

We believe that legislation currently being enacted in USA and in Europe runs a significant risk of criminalising the vendor-independent security vulnerability analysis of software products. We seek to ensure that, in the public interest, the freedom to perform this essential service is enshrined in European legislation.

Summary

[1] a high incidence of security-related software flaws contributes significantly to e-crime against business, by rendering software products, and the increasingly essential services they provide, vulnerable to abuse by the criminal fraternity[2].

[2] product vendor spokesmen have declared the elimination of such flaws by themselves to be uneconomic[3].

[3] a substantial community of vendor-independent software experts currently contributes to the analysis and reporting of such flaws.

[4] this independent analysis and reporting service is broadly provided on a not for profit basis for the public good.

[5] to analyse products for security flaws, it is necessary to reverse engineer them.

[6] discovered vulnerabilities must be reported openly to the user community in a timely manner to allow solutions to be implemented.

[7] a combination of new technological departures and new legislation is likely to criminalise the performing of these activities by the independent security community.

[8] we must ensure that European and UK law formally enshrine the continued freedom to perform independent software product security analysis and vulnerability reporting for the common good.

[9] we propose that this matter be placed on the EURIM agenda for full discussion.

[1] "security research exemption to DCMA considered", Kevin Poulsen, Security Focus News. www.securityfocus.com/news/4729
[2] http://icat.nist.gov/icat.cfm
[3] Andy Cobbold, BMC. Quoted in "Suppliers hit back over software quality". Computer Weekly 24/06/2003. p16.

Discussion

Law, USA - Digital Millennium Copyright Act

The Digital Millennium Copyright Act (DMCA) (USA HR.2281)[4] was enacted in 1998, essentially as an anti-piracy measure *"... after fierce lobbying from the motion picture and recording industries ..."*[5] and the Act makes it unlawful to circumvent *"... effective technological measures that are used by authors in connection with the exercise of their rights under this Treaty or the Berne Convention and that restrict acts, in respect of their works, which are not authorized by the authors concerned or permitted by law."* for any purpose, subject to some limited exceptions.

There have already been several attempts to invoke the Act to restrict freedoms that were previously available under copyright laws.

In 2001 Edward Felten, a respected Princeton computer science professor, took up a music industry body challenge to attempt to crack an encryption system for music files. Having succeeded, he declared his intention to present his results at an academic conference. At this point, the body in question threatened action under DMCA[6].

Dmitri Sklyarov was arrested on a criminal charge in July 2001, for developing a product that converts Adobe e-Books into PDF format. Adobe considered this to infringe their IPR as protected by DMCA, although copyright infringement was not alleged. This was the first action brought in connection with software development under DMCA[7].

These cases, high-profile as they are, did not demonstrate whether the Act precludes independent reverse engineering of software, and that matter is still in dispute. It would seem *prima facie* that unless the software were in some way protected by *"effective technological measures"*, DMCA would not apply. However, there have been several attempts so far to invoke DMCA where the software was not so protected.

Typical is the dispute between Hewlett Packard and SnoSoft. In July 2002, SnoSoft, a loose consortium of vulnerability researchers, discovered numerous security vulnerabilities in a Hewlett Packard product. Hewlett Packard threatened to invoke DMCA against them[8,9], although the product was not protected by any effective technological measures. HP based their threat of action on a presumed right to control the means by which the vulnerabilities were disclosed, rather than on any circumvention or act of reverse engineering. The threat was subsequently retracted by HP[10,11], at which time it made an interesting explicit statement *"unlike its counterpart Adobe Systems, it will not use the protection provided by the provisions of DMCA as it would stifle research and impede the flow of information"*[12]. The mention of Adobe refers to the Sklyarov case, which is not strictly relevant, as that case rested on the creation of a software tool by Sklyarov, rather than on the mere disclosure of information.

More recently, Blackboard Inc. have invoked the DMCA to prohibit Hoffman and Griffith presenting a conference paper about security flaws in one of its products[13].

[4] http://www.educause.edu/issues/dmca.html
[5] www.securityfocus.com/news/4729
[6] www.cs.princeton.edu/sip/sdmi/faq.html
[7] www.eff.org/IP/DMCA/US_v_Elcomsoft/us_v_sklyarov_faq.html
[8] news.com.com/2100-1023-947325.html
[9] www.politechbot.com/docs/hp.dmca.threat.073002.html
[10] www.pcworld.com/news/article/0,aid,103853,00.asp
[11] mail.lab.net/lists/archive/politech-exploder/2002-August/001655.html
[12] www.asianlaws.org/cyberlaw/archives/08_02_hp.htm
[13] www.theregister.co.uk/content/archive/30259.html

In spite of great controversy[14] aroused by these and similar cases (most of which incidentally seem ultimately to fail), security researchers are getting the message that should they continue to investigate and publish security vulnerabilities of commercial software, they face the prospect of crippling law suits which the vendor can afford to prosecute, but they cannot afford to defend.[15]

Nevertheless, while this controversy continues, a number of US states are in the process of enacting legislation[16] that further extends the powers of DMCA to prohibit a wide range of specific acts, including in some cases the use of well-established network perimeter security measures.

The Association for Computing Machinery (ACM) has recently attempted to introduce an amendment to DCMA that would explicitly exempt the breaking of copy protection schemes *"that fail to permit access to recognize shortcomings in security systems, to defend patents and copyrights, to discover and fix dangerous bugs in code, or to conduct forms of desired educational activities"*[17]. In this regard, Barbara Simons of the ACM said *"I'm going to argue that the [current] exemptions aren't sufficient, because we're having security people threatened"*[18]. Whether this attempt is successful remains to be seen, but it is a significant pointer to the way forward for European legislation.

Law, Europe - Directive 2001/29/EC

"Directive 2001/29/EC ... on the harmonisation of certain aspects of copyright and related rights in the information society" nominally[19] became law on 22/12/2002. It seems essentially modelled on DMCA, and appears to have the same flaws. Particularly, the legal definition of a *"technical protection measure"* is open ended, leaving the industry free to make its own mind up as it goes along. In consequence, a new *sui generis* intellectual property right has been invented: the right to control access to works wholly independently of whether copyright subsists in those works. The right is not subject to copyright exemptions *per se*, nor is it (or could it be) subject to the traditional intellectual property balancing factors such as term. We could therefore be considered to be following the American lead, regardless of the very just and reasonable controversy it has aroused in USA.

Law, UK - Copyright Designs and Patents Act 1988

By defining it as *"not fair dealing",* section 29(4) of the CDPA makes it an offence to decompile a software program: that is, *"to convert a computer program expressed in a low level language into a version expressed in a higher level language"* or *"incidentally in the course of so converting, to copy it"*. This definition effectively prevents any reverse engineering of software programs, as in order to examine computer programs it is normally essential to convert the numeric machine codes of the executable program into some human-understandable mnemonic equivalent. The sole permitted exception is provided by section 50B, which permits these acts where the objective is *"to obtain the information necessary to create an independent program which can be operated with the program decompiled or with another program"* (to achieve interoperability), and explicitly that "*the information so obtained is not used for any purpose other than the permitted objective"*. Clearly, reverse engineering to find or research security vulnerabilities is expressly excluded from this exception.

[14] www.eff.org/IP/DMCA/20030102_dmca_unintended_consequences.html
[15] news.com.com/210001001-272716.html
[16] www.freedom-to-tinker.com/superdmca.html
[17] www.securityfocus.com/news/4729
[18] ibid.
[19] At that time it lacked the necessary EP co-decision

Section 29 provides for exemption for "research or private study": however, since the 1992 introduction of s50B[20] as a **permitted act** the s29 **exemption** explicitly no longer extends to reverse engineering[21]. The available literature[22], though mentioning this connection while arguing for law reform, entirely misses the significance of this distinction. With some irony we may observe that the legal lacuna thus introduced amounts to a criminal's charter: its effect on security is to hamper only those, including not only researchers but also the civil authority, endeavouring to stop those already disregarding the law.

Trusted Computing Platform Architecture

When we additionally take into account the market drive towards TCPA (Trusted Computing Platform Architecture)[23], typified by Microsoft's Palladium project, the picture gets considerably worse. The concept of TCPA is that all computing resources, be they hardware, software or data files, will be "digitally signed", and that validation of the digital signatures will be performed in real time over the Internet when the resources are used. Quite apart from the unprecedented control this will hand to vendors over continued use of resources, it will explicitly apply *"effective technological measures"* within the current interpretation of DMCA (and possibly Directive 2002/29/EC) to all computing resources, criminalising the circumvention of these. As the circumvention of this signing would be a necessary prerequisite to any vulnerability analysis, it would not be possible for any independent researcher to examine the internals of any computing resource without committing an offence.

Furthermore, the very complexity of TCPA as envisaged by the TCPA Consortium and Microsoft, the inventor of the Palladium operating system software used to control TCPA enabled computers, and the resulting reliance of every computer user on the continued accessibility of a vast mesh of remote certification servers will increase the significance of software vulnerabilities where they occur. We will therefore have all the greater need of the community of independent vulnerability researchers, whom legislation is likely to eliminate.

Open Source software such as the thriving Linux operating system is also threatened. Once TCPA-enabled, as it will have to be in order to share information resources, the very concept of open source is void should the circumvention of *"effective technological measures"* remain an offence.

Conclusions

As e-government becomes a global reality across Europe, we must not allow ourselves to bow to commercial vested interests at the expense of the public. This possibility is not new, nor is it restricted to the computing arena. However, in the UK the common-law judicial leeway to break intellectual property in favour of public policy remains intrinsically very weak. A classic example of the potential problems is provided by Lion Laboratories v Evans[24]. In that case, the decision was for the nominally infringing defendants, with Stephenson LJ concluding *"...we must not restrain the defendants from putting before the public this ... information"*. However, Griffiths LJ cautioned: *"…if [the court is] convinced that a strong case [of public interest] has been made out, the press should be free to publish, leaving the plaintiff to his remedy in damages"* (emphasis added). Thus the public interest defence for publication of security vulnerabilities is severely circumscribed by the very credible threat of damages for loss of profit – especially as this case came to rest in the Court of Appeal.

[20] Noted, as curiously anticipating the US case *Sony v Connectix* , 203 F3d 596 (9th Cir. 2000) and DMCA s1201(f), by D. Rowland and A. Campbell, *Supply Of Software: Copyright And Contract Issues*, [2002] IJL&IT 10(23)

[21] Exemptions apply to any user; whereas permitted acts apply only to **lawful** users, i.e. licencees.

[22] Rowland and Campbell, *op cit*.

[23] Wobst, R. The Golden Cage: TCPA, Palladium and Some Likely Market Consequences. Information Security Bulletin. 8,3, 2003.

[24] *Lion Laboratories v Evans* [1984] 2 AII E.R. 417, CA, quoted in Cornish W. Cases and Materials on Intellectual Property. London. Sweet & Maxwell, 2003.

The enactment of DMCA and the adoption of harmonised legislation in Europe is troubling in the context of independent software product security research. The legislation has already been used to stifle open disclosure that was arguably in the public interest. Whether or not proceedings are in general successful, the threats of civil action, and indeed criminal prosecution, can only serve to deter the independent research community from providing an essential service for the common good that software vendors have conclusively shown themselves unable or unwilling to perform. We therefore propose that explicit rights at least as generous as the proposed ACM amendment to DMCA be enshrined in European and UK law.

END