Daniel McEnnis

Proposal to exempt source code from protection under the anti-circumvention clause of the DMCA where source code is defined as a human readable description and/or defintion of the behavior of a computer program that can be transformed into a format executable by a computer but effectively unreadable by humans.

Summary of argument:

The encryption of source code renders researchers liable if they choose to alert system administrators of critical security flaws in software that permit outside attackers to seize control their systems. Not only does this stifle legitimate scholarship, it prevents system administrators from developing counter measures to protect their systems against outside attack. In particular, it undermines efforts to secure the US's internet infrastructure against hostile attacks by terrorists and rogue states by preventing the legal dissemination of the knowledge needed to defend against these attacks.

Argument:
Technological measure- Source code rendered into binary form effectively encrypts the source code.

Non infringing use prevented - evaluation of the security of software packages. In particular, security audits assessing the likelihood that unauthorized users can utilize installed software to illegally hijack the resources of the computer system in which this software is installed.

How this circumvents the encryption - the testing process unencrypts portions of the binary translation by describing any potentially dangerous and/or subversive behaviors the software possesses that may pose a threat to system integrity.

Why this is otherwise protected - "Clean room" implementations of software (precise descriptions of software behavior which exactly duplicate the behavior of another system created without access to the original software's unencrypted content) are protected under fair use (IBM lawsuit to prevent i386 clones). In addition, the quoting of portions of content for reporting purposes is explicitly permitted under fair use doctrine.

Harm 1- Encourages non-US security researchers to explicitly prevent US citizens from accessing their work. (See RedHat advisory board for RHLinux for details of one such example (1)) This is done to protect researchers in countries that do not accept the validity of the DMCA within their borders from potential lawsuits in the US. This places US system administrators at a disadvantage against potential attackers since they are denied access to descriptions of how attackers can hijack their systems resources (preventing the deployment of countermeasures) while criminal attackers have full access.

Harm 2- Discourages prompt reporting of system flaws to system administrators. Since those reporting flaws can experience (and have been threatened with) legal retaliation by software manufacturers, there is a significant disincentive to provide the information necessary to enact effective countermeasures. These information disclosures are typically unpaid. When a significant potential financial burden is attached, the rewards of providing the needed information are dwarfed by potential liabilities.

Harm 3- Encourages complacency by software providers. Prior the DMCA's circumvention provision, companies with defective software were compelled by bad publicity to release well-tested patches quickly. Evidence provided below indicates that at least some companies are abusing the DMCA's anti-circumvention clause to prevent their customers from discovering their vulnerability to criminals by threatening legal action against those individuals who publish this information(2).

Harm 4- Recent reports from the Bush administration have reaffirmed the role rank and file system administrators have in securing the nations internet infrastructure against assault by terrorist organizations and rouge states. The DMCA's circumvention clause in relation to source code provides a significant hindrance to protection of the internet from hostile attack. System administrators are not only highly decentralized, but are scattered throughout a wide range of private and public enterprises. Effectively disseminating the information necessary to predict and prevent large scale assaults on the infrastructure are only possible if the information needed to prevent these assaults is protected against legal retaliation. Evidence that this threat is real is provided by the recent large-scale assaults against the DNS root servers in the past month (3).

Specific examples cited in this work-

(1)Descriptions of vulnerabilities discovered in software packages utilized in the Red Hat Linux operating system are published by foreign researchers in a fashion that bars US citizens from accessing this information. The researchers explicitly state that their decision to ban access by US citizens was motivated by fears of legal retaliation in the US under the DMCA's anti-circumvention clause.

(2)On July 19, 2002 HP sends legal notice to Adriel T. Desautels of Secure Network Operations, Inc. that they intend to prosecute under the DMCA's circumvention clause unless they make every possible effort to retract publication of the security flaws in HP's True64 Unix operating System – full text of this letter provided below.

Sophisticated attack against dns root servers - Recently, a massive denial of service attack was launched against the 'root dns' servers - those computers that provide the means to translate word based internet addresses into raw IP addresses. The attack was both of exceptionally sophisticated and conducted in a manner suggesting of a test. The system was attacked for a brief time, then the attack was stopped by the attacker before the underlying structure of the internet could be significantly degraded. Both the unusually high degree of sophistication in the attack and the exploratory nature of the attack lend

credibility to the threat of a future sophisitcated large scale assault against critical internet resources on which the economy is now dependant.

July 29, 2002

By Electronic and Certified Mail

Adriel T. Desautels

Secure Network Operations, Inc.

D/B/A SnoSoft

5 Oak Ridge Drive, Apt. # 2

Maynard, MA 01754

Re: Tru64 UNIX Buffer Overflow Exploit

Dear Mr. Desautels:

It has been brought to my attention that, on July 18, 2002, a buffer overflow exploit of Tru64 UNIX was posted on securityfocus.com under the alias phased@webtribe.net (a/k/a "phased", phased@mail.ru" and "James Green"). Based on information provided by Gil Novak to HP concerning aliases utilized by SnoSoft, we understand that this action was taken by an agent of SnoSoft despite SnoSoft's representations that it intended to comply with the industry standard practice of reporting its findings to CERT and despite the ongoing discussions between Gil Novak and Rich Boren on this issue.

Please be advised that the posting of the buffer overflow exploit has exposed SnoSoft and its members to potential federal criminal liability under both the Digital Millennium Copyright Act ("DMCA") and the Computer Fraud and Abuse Act. Under the DMCA, SnoSoft and its members could be fined up to $500,000 and imprisoned for up to five years for "offering to the public . . . any technology . . . that is primarily designed or

produced for the purpose of circumventing protection afforded by a technological measure that effectively protects a right of a copyright owner." See 17 U.S.C. § 1201(b). In addition, under the Computer Fraud and Abuse Act, if anyone uses the buffer overflow exploit posted by SnoSoft on securityfocus.com to cause damage to a Tru64 UNIX system, SnoSoft and its members could be subject to significant criminal sanctions, including up to ten years in prison. See 18 U.S.C. § 1030(c)(3) & (4). Finally, SnoSoft and its members may face additional penalties under various criminal statues of the Commonwealth of Massachusetts including, but not limited to, criminal extortion (M.G.L. c. 265 § 25).

HP hereby requests that you cooperate with us to remove the buffer overflow exploit from securityfocus.com and to take all steps necessary to prevent the further dissemination by SnoSoft and its agents of this and similar exploits of Tru64 UNIX. If SnoSoft and its members fail to cooperate with HP, then this will be considered further evidence of SnoSoft's bad faith. Finally, HP also reserves its right to seek whatever legal recourse it has against SnoSoft and its members for monies and damages caused by the posting and any use of the buffer overflow exploit

Regards,

Kent Ferson

cc: Gil Novak

bcc: David Cardos

Rich Boren