Questions to Establish Potential Chilling Effects of the Digital Millenium Copyright Act (DMCA) on the Conduct of Computer Security Research

Information Security and Privacy Advisory Board
(previously the Computer System Security and Privacy Advisory Board)
January 2003

Background and Introduction

The Computer System Security and Privacy Advisory Board was created by the Computer Security Act of 1987 (P.L. 100-35) to examine issues affecting the security and privacy of sensitive (unclassified) information in federal (Executive Branch) computer and telecommunications systems. Under new legislation, The Federal Information Security Management Act of 2002, the Board was renamed the Information Security and Privacy Advisory Board.

The Board's responsibility includes providing advice on computer security and privacy matters. Issues affecting research performed by Federal agencies or under Federal agency auspices, where research pertains to computer security or privacy, fall under the Board's purview. Legislation, regulations, and judicial actions that may affect the conduct of computer security research, and especially those actions with the potential to restrict such research, or limit its quality, or have a chilling effect on the commencement of research, are areas of Board interest and concern.

The Board is committed to ensuring that any adverse impact on research supporting computer security and privacy be identified and understood, so legislators and decision-makers can make fully informed decisions as to whether an encumbrance on such research is justified. The Board's view is that accomplishing strong computer security requires strong computer security research

In this context, the Board reviewed the Digital Millennium Copyright Act (DMCA) (Public Law 105-304, 1998). Based on its review, the Board has several concerns about how the Act may affect computer security research and ultimately affect the security of Federal computer systems.

This paper lists the Board's concerns and identifies questions which the Board believes should be considered and, if possible, answered to establish what effects the Act is or may have on computer security research.

Section 1201 of DMCA

The primary focus of concern is Section 1201, specifically the provisions that prohibit the development of technology to circumvent, defeat, or undo copyright protection schemes. The law provides for criminal and civil penalties for noncompliance. However, several

provisions in Section 1201 may have the perverse effect of limiting security research, even that done by, or on behalf of, the Federal Government.

To understand these concerns, it is helpful first to recite the Section 1201 exclusion in paragraph (e):

> "This section does not prohibit any lawfully authorized investigative, protective, information security, or intelligence activity of an officer, agent, or employee of the United States, a State, or a political subdivision of a State, or a person acting pursuant to a contract with the United States, a State, or a political subdivision of a State. For purposes of this subsection, the term "information security" means activities carried out in order to identify and address the vulnerabilities of a government computer, computer system, or computer network."

The following sections describe the concerns associated with Section 1201 and this exclusion.

Definition of "information security"

The definition of "information security" in Section 1201 paragraph (e) seems to indicate that this area covers only a quest for "vulnerabilities" (a term which is also not further defined). This view is extraordinarily narrow. In fact, information security covers a much broader scope, including research on improving the efficiency of information security measures (which affects their adoption and use), and research to determine whether security measures create technical conflicts with other computer system features. Additionally, the language could be read to apply only to known vulnerabilities, not to unknown or potential ones.

The Board therefore poses the question, does the way the exemption language is crafted unduly restrict the ability of both public and private entities to perform or sponsor computer security research?

Narrowness of Exemption

The paragraph (e) exemption for Federally-sponsored research appears to be narrowly drawn. Section 1201 excludes computer security research and work done for or by the Federal government excepting "dual use" technologies (i.e., those for which there are legitimate research needs, stemming from government or non-government applications, but which also may be employed to circumvent, defeat or undo copyright protection schemes). It includes only a narrow exemption for encryption research.

The Board therefore poses the question, is the Section 1201 paragraph (e) exemption too narrowly drawn with respect to dual use technologies or encryption?

Dual-use technologies

The Act gives little consideration to dual-use technologies. Technologies exist for which there are legitimate research needs stemming from government or non-government applications, and which also may be employed to circumvent, defeat, or undo copyright protection schemes. Such technologies include protocols that convey security-related information and mathematical processes that can be used to analyze analog or digital signals (or the representation of those signals in electro-magnetic or optical storage media) for evidence of tampering or the presence of covert channels to convey information (including steganography, or information hiding). Such processes have a multitude of uses, including evaluating how copyrighted information is stored on electro-magnetic or optical media. Such research could lead to removing or defeating "digital watermarking." Yet these are important topics to computer security and establishing how well information or systems may be protected from unauthorized access or modification.

The Board therefore poses the question, does the current statutory language have a chilling effect on research into areas of vital importance to computer security, as cited above?

Lack of process for researchers to show their intent

The Board observes that no specific process has been established, or is required to be established under the Act, for researchers to demonstrate that their results are not intended for circumventing, defeating, or undoing copyright protection schemes.

Section 1201 provides a limited exception for encryption researchers, determined by "whether the person is engaged in a legitimate course of study, is employed, or is appropriately trained or experienced, in the field of encryption technology." Because a number of encryption and security researchers possess educational or professional backgrounds in other non-encryption disciplines, such as mathematics, it is unclear whether they would be considered to fall into any of the "encryption technology" categories enumerated in the statute. Moreover, it is unclear who would make this determination; and the lack of such certainty must itself create uncertainty in the minds of those desiring to perform such research. Hence, the scope and interpretation of the Section 1201 exemption are uncertain.

From discussions with researchers, the Board observes that there is real and considerable uncertainty and confusion on this matter. Such confusion can have a chilling effect on research. The Board is unaware of any process or any written legal interpretation or any other written guidelines that define the individuals who qualify under this exception.

The Board therefore poses the question, does the "researcher" exemption in the Act warrant clarification, elaboration, and/or expansion to ensure that computer security research is not unknowingly or unduly chilled?

Need for consent of copyright owner

Another point of concern is whether or not, and under what circumstances, the consent of a copyright owner must be obtained before performing research, as set forth in Section 1201 paragraph g(2)(C). Because of the ambiguity of this paragraph and the lack of a described process for obtaining permission, the implication is that each copyright owner may establish his or her own process, and may demand information from an applicant which is inappropriate or intended to chill the research rather than reasonably provide consent. Such behavior could be a barrier for researchers.

The Board therefore poses the question, does the language in the Act concerning getting the consent of copyright owners as a prerequisite for research warrant clarification or elaboration to ensure that both researchers and copyright owners have a clear understand of the process which the Act prescribes?

Limiting fields of study

The Board has considered whether or not the DMCA will affect the fields of study that Ph.D. students choose for research. No normative data apparently exists to show whether this concern has merit; however, the lack of data may be a reflection of the security research community confusion over the Act's language. If the Act has affected the choice of study, this, too, will have a chilling effect on students entering the field and will have a corresponding limiting effect on research in that field.

The Board therefore poses the question, is there evidence that the DMCA is affecting what fields of research Ph.D. students are selecting relevant to computer security, and if there is no useful data on this point, would it be useful to obtain some?

Lack of case law

The Board is unaware of any Federal or state case law which deals with the scope or impact of the DMCA, and especially how it applies to computer security research on dual-use technologies, even where the research is not intended to or undertaken for the purpose of circumventing, defeating, or undoing copyright protection schemes. It would be useful to track any such litigation to determine whether the outcome will adversely affect computer security research.

The Board therefore poses the question, would it be worthwhile for the Act to be modified to require periodic evaluations by NIST of any case law that may develop, to determine whether courts are interpreting the language of the Act in a fashion which is impeding computer security research?

Copyright protection algorithms and technologies

The Board sees a need for determining whether the algorithms and/or technologies developed specifically for copyright protection are secure and technically sound, especially in view of past experience with proprietary mechanisms that lacked sufficient technical review and were proven to be fatally flawed. In particular, the Board believes there is a need for independent analyses of these copyright protection algorithms/technologies, yet it is unaware of any such analyses. Among others, this concern is pertinent to the U.S. Patent and Trademark Office which may need to make determinations on these points for the purpose of granting patents.

The Board, therefore, poses the question, how should copyright protection algorithms/technologies be independently evaluated so as to establish their technical soundness and to support evaluations by the Patent and Trademark Office?

.