Name and Affiliation

I am Shawn Hernan, a senior member of the technical staff at the CERT Coordination Center (CERT/CC). CERT/CC is part of the Software Engineering Institute, a federally funded research and development center operated by Carnegie Mellon University and dedicated to improving the state of the practice of software engineering. The following comments are submitted on behalf of the CERT/CC.

Proposed Class(es) of Works

1. Those literary works, musical works and audiovisual works, for which a person has lawfully obtained a right of use, protected by access control mechanisms which include features, flaws or vulnerabilities that (a) expose (i) the works to be protected or (ii) other assets of the users of such measures--including computers, computers systems or computer networks or the data or other protected works used with them--to infringement, compromise, loss, destruction, fraud and other adverse actions or (b) permit the privacy of such users to be compromised.

2. Those literary works representing computer software programs and databases, for which a person has lawfully obtained a right of use, that operate to control access to works protected under the Copyright Act but contain features, flaws or vulnerabilities that (a) expose (i) the works to be protected or (ii) other assets of the users of such measures--including computers, computers systems or computer networks or the data or other protected works used with them--to infringement, compromise, loss, destruction, fraud and other adverse actions or (b) permit the privacy of such users to be compromised.

3. Compilations consisting of lists of websites blocked by filtering software applications.

4. Literary works, including computer programs and databases, protected by access control mechanisms that fail to permit access because of malfunction, damage or obsoleteness.

Summary of the Argument(s)

1. Access control mechanisms that fail to provide adequate security to the works they are intended to protect are also likely to expose the authorized user of a computer, computer system, or network to damage or loss, including the loss of privacy. The presence of these flawed mechanisms exposes other protected works on related computers, computer systems, and networks, to unauthorized access. The requested exemption permits those with a lawful right of access to conduct additional research, scholarship and criticism regarding the adequacy of the control mechanisms, as well as protected works, within the scope of fair use. Prohibiting circumvention relating to the proposed exempt class of works is estimated to cost the American economy significant amounts per year (although precise cost estimates are, for a variety of reasons including underreporting of losses and the existence of indirect losses, virtually impossible to ascertain) due to (a) unauthorized access through defective control mechanisms, (b) costs incurred by consumers and businesses to repair features, flaws or vulnerabilities in such control mechanisms and (c)

lost revenues from users who avoid expenditures on protected works and related computer-based expenses out of concern for security and privacy risks associated with the related access controls. The proposed exemption will have no adverse impact upon the owners of the classes of works for which the exemption is requested.

2. Computer software programs and databases that operate to control access to works protected under the Copyright Act can contain features, flaws or vulnerabilities that expose the computers, systems, networks and other assets of authorized users to damage or loss, including the loss of privacy. In furtherance of the exemptions relating to circumvention available under Section 1201(e), 1201(g) and 1201(j), the proposed exemption permits authorized users to vigorously research, test and verify the functionality of the class of works to which the proposed exemption relates, and to publish related results and criticisms regarding such works, within the scope of fair use. The costs of prohibiting circumvention of the proposed exempt class of works are enormous. The failure to be able to test, and subsequently remediate, security flaws in software and databases is estimated to cost the American economy significant dollar amounts per year due to (a) unauthorized access through defective control mechanisms, (b) costs incurred by consumers and businesses to repair features, flaws or vulnerabilities in such control mechanisms and (c) lost revenues from users who avoid expenditures on protected works and related computer-based expenses out of concern for security and privacy risks associated with the related access controls. These costs are matched by the continued risks of substantial harms not yet realized from future adverse events related to the inability to circumvent and test access controls protecting the class of work.

3. The proposed exemption is fully supported by the rationale adopted by the Register in the initial exemption rulemaking under Section 1201(1)(a)(3). There have been no changes in the marketplace or in the related technologies or business practices that mitigate against the necessity for continuing the exemption.

4. The proposed exemption is fully supported by the rationale adopted by the Register in the initial exemption rulemaking under Section 1201(1)(a)(3). There have been no changes in the marketplace or in the related technologies or business practices that mitigate against the necessity for continuing the exemption.

Argument in Support

Proposed Exemption No. 1.

Class of Works

The proposed exemption includes those literary works, musical works and audiovisual works, for which a person has lawfully obtained a right of use, protected by access control mechanisms which include features, flaws or vulnerabilities that (a) expose (i) the works to be protected or (ii) other assets of the users of such measures—including computers, computers systems or computer networks or the data or other protected works used with them—to infringement, compromise, loss, destruction, fraud and other adverse actions or (b) permit the privacy of such users to be compromised.

The Register of Copyrights and the Librarian of Congress have previously recommended an exemption for a class of works represented by literary works, including computer programs and databases, protected by access control mechanisms that fail to permit access because of malfunction, damage or obsoleteness. See 65 Fed. Reg. 64,555 (October 27, 2000). The proposed new exemption is intended to take into account substantial advances that have occurred in both the technological measures that are employed to control access to protected works and, as well, the increased sophistication of technologies and procedures through which the security and integrity of computers, computer systems and computer networks, and the privacy of individual users, can be compromised.

The proposed exemption expands upon the scope of the previous exemption by recognizing additional classes of works. The addition of musical works and audiovisual works reflects the increased multi-media quality of computer-based materials that are entitled to protection under the Copyright Act. However, the essential premise of the new exemption remains consistent—by permitting those who have a lawful right of access to the exempted class of works to circumvent controls that present security risks, the overall legislative objective of achieving high-quality and properly functional technological measures can be advanced.

Technological Controls

The proposed exemption is specifically associated with specific technological measures with respect to which circumvention should not be prohibited. Those technological measures are those access control mechanisms which include features, flaws or vulnerabilities that (a) expose (i) the works to be protected or (ii) other assets of the users of such measures—including computers, computers systems or computer networks or the data or other protected works used with them—to infringement, compromise, loss, destruction, fraud and other adverse actions or (b) permit the privacy of such users to be compromised.

Access control mechanisms that fail to provide adequate security to the works they are intended to protect, even if working as intended, should not place users at undue risk. In this sense, such access control mechanisms are analogous to mechanisms that fail due to malfunction, damage or the passage of time; in each instance, the expectations of those authorized to access the protected works can be defeated. However, access control mechanisms that include features, flaws or vulnerabilities that present security risks involve more than a frustrated expectation of being able to properly access the protected class of works. They also expose to loss other, often significant, assets of the users—computers, computer systems, computer networks, other protected works (such as licensed applications or content) and data. Losses can be in the form of infringement, impaired functions, denial of service, fraud, destruction, alteration and similar adverse events. In addition, access control mechanisms that present security risks place the privacy of users at risk—features, flaws or vulnerabilities that permit the undisclosed monitoring of usage, the tracking of computer services, the exposure of personal financial, medical or similar information can all be associated with technological measures that exist to protect against or control access. The danger with respect to all such features, flaws or vulnerabilities (and one of the central harms this proposed exemption seeks to remedy) is that users may be unaware of the risks to critical assets that the use of such software may introduce. The proposed exemption would allow the continuation of research that brings these problems to users' attention so that they may remediate the problems or otherwise seek to manage the risks presented.

Prevented Activities

The proposed exemption permits those users otherwise authorized to access the protected works to research, challenge, test and otherwise stress the functionality and features of these technological controls to determine if they possess features, flaws or vulnerabilities presenting security and privacy risks. This conduct involves legitimate and fair uses of the protected works (and the related access controls). The research itself can produce scholarship and criticism that, when published, represents fair use within existing copyright law and is otherwise non-infringing upon the classes of work for which the exemption is proposed.

Users should be permitted to circumvent or attempt to circumvent those controls where such conduct exposes features, flaws or vulnerabilities that present such risks. In the absence of the exemption, this type of research, scholarship and criticism cannot be lawfully conducted without risking violation of the prohibition against circumvention established by Section 1201(a)(1)(A). As a consequence, control mechanisms (even those that may function properly at controlling access) can be introduced into commerce that present to users significant and material security and privacy risks.

The proposed exemption is entirely consistent with the strong commitment made by the Digital Millennium Copyright Act to exempt from the Act's prohibitions various activities that advance the security and trustworthiness of digital protected works. Those exemptions include those set forth in Sections 1201(e) ("information security" conducted under certain government contracts), 1201(g) ("encryption research") and 1201(j) ("security research"). The exemption serves to assure that security-based research, scholarship and criticism of the proposed classes of works that involves the circumvention of the related controls to demonstrate the existence or extent of features, flaws and vulnerabilities is not treated as prohibited conduct, even where such research is not covered by another exception to 1201(a)(1)(A)'s general prohibition.

The academic and business community has made substantial investments in improving the security and privacy associated with the use of digital works protected by copyright. Independent research firms, consultants and academic institutes regularly engage in the testing of properly licensed works in order to determine the existence of security-based features, flaws or vulnerabilities. This activity produces ongoing reports to the vendors and service providers associated with the works, to the users themselves and to the general public regarding the existence of such features, flaws or vulnerabilities. These reports help contribute to the adoption of continuing improvements that enhance the security of digital properties and services and improve the ability to protect the privacy of users against unexpected losses.

It is important to emphasize that the security-based research, scholarship and criticism otherwise prevented in the absence of the exemption is activity that would be conducted by those with a lawful right of use regarding the protected works. No "hacking," "cracking" or unlawful attacks are intended to be authorized or permitted by the proposed exemption.

Related Harms

Prohibiting circumvention relating to the proposed exempt class of works is estimated to cost the American economy significant dollar amounts per year (although precise cost estimates are, for a variety of reasons including underreporting of losses and the existence of indirect losses, virtually impossible to ascertain) due to (a) unauthorized access through defective control mechanisms, (b) costs incurred by consumers and businesses to repair features, flaws or vulnerabilities in such control mechanisms and (c) lost revenues from users who avoid expenditures on protected works and related computer-based expenses out of concern for security and privacy risks associated with the related access controls.

Some specific data is available from the Computer Security Institute's "2002 Computer Crime and Security Survey." The Computer Security Institute conducts its annual survey with assistance from the San Francisco FBI's Computer Intrusion Squad. Data from the 2002 survey includes:

- Ninety percent of respondents (primarily large corporations and government agencies) detected computer security breaches within the last twelve months.

- Eighty percent acknowledged financial losses due to computer breaches.

- Forty-four percent (223 respondents) were willing and/or able to quantify their financial losses. These 223 respondents reported $455,848,000 in financial losses.

- As in previous years, the most serious financial losses occurred through theft of proprietary information (26 respondents reported $170,827,000) and financial fraud (25 respondents reported $115,753,000).

- For the fifth year in a row, more respondents (74%) cited their Internet connection as a frequent point of attack than cited their internal systems as a frequent point of attack (33%).

With respect to many, if not most, of these losses, the intrusion or damage was made possible by the exploitation of a feature, flaw, or vulnerability within the proposed class of protected works.

Effects of the Proposed Exemption:

The proposed exemption will have no adverse impact upon the owners of the classes of works for which the exemption is requested. It will have several positive effects:

1. Effect on Availability

Unless the proposed exemption is granted, many of the technological measures that would otherwise be capable of exempt circumvention may be inaccessible to the research activity that is contemplated.

2. Effect on Criticism, Comment, and News Reporting

The proposed exemption will have a positive effect on criticism, comment, and news reporting by better assuring that threats of DMCA violations will not stand as a barrier to the evaluation of software security flaws.

3. Effect on Teaching, Research, and Scholarship

The proposed exemption will have a positive effect on teaching, research, and scholarship. The availability of independent research on existing software flaws directly aides and promotes teaching and scholarship by adding to the existing body of knowledge concerning software technology and products.

4. Effect on the Market

The proposed exemption will have a long-term beneficial effect on the market. The use of protected works in digital form is likely to be improved in an environment where flaws can freely be identified, discussed, and remediated. Awareness in the marketplace that products will be independently tested and flaws identified and remediated will tend to increase market confidence in such products. To draw an analogy, the crash testing of automobiles, over time, has resulted in safety improvements that have in turn led to increased market acceptance of automobiles and increased the value of products incorporating lessons drawn from such testing.

5. Effect on Copyright Owners

The proposed exemption will have no effect on the rights of copyright holders. The proposal is limited to legally acquired protected works (including demonstration and trial versions).

Proposed Exemption #2

Class of Works

Those literary works representing computer software programs and databases, for which a person has lawfully obtained a right of use, that operate to control access to works protected under the Copyright Act but contain features, flaws or vulnerabilities that (a) expose (i) the works to be protected or (ii) other assets of the users of such measures—including computers, computers systems or computer networks or the data or other protected works used with them—to infringement, compromise, loss, destruction, fraud and other adverse actions or (b) permit the privacy of such users to be compromised.

Technological Controls

The works included within the proposed exemption include technological measures that limit access to such works. These access controls can present risks to privacy and security by including features, flaws or vulnerabilities that present two targets of exposure: (i) the works that are protected by such measures against improper access and (ii) other assets of the users—including computers, computers systems or computer networks or the data or other protected works used with them. Even if the access controls function as designed, they can present security risks which, if not identified (including by testing and circumvention), present the opportunity for catastrophic losses involving compromise, destruction, alteration, infringement, fraud and similar adverse actions. In addition, certain features, flaws or vulnerabilities can compromise the privacy of the users.

Prevented Activities

The proposed exemption permits users otherwise authorized to access the programs and databases to research, challenge, test and otherwise stress the functionality and features of their technological controls to determine if they possess features, flaws or vulnerabilities presenting security and privacy risks. This conduct involves legitimate and fair uses of the protected works (and the related access controls). The research itself can produce scholarship and criticism that, when published, represents fair use within existing copyright law and is otherwise non-infringing upon the programs, databases or technological controls.

Users should be permitted to circumvent, or attempt to circumvent, those controls where such conduct exposes features, flaws or vulnerabilities that present such risks. In the absence of the exemption, this type of research, scholarship and criticism cannot be lawfully conducted without risking violation of the prohibition against circumvention established by Section 1201(a)(1)(A). As a consequence, control mechanisms (even those that may function properly at controlling access) can be introduced into commerce that present to users significant and material security and privacy risks. Since no other available statutory exemption permits such conduct, the proposed exemption is necessary.

The proposed exemption is entirely consistent with the strong commitment made by the Digital Millennium Copyright Act to exempt from the Act's prohibitions various activities that advance the security and trustworthiness of digital protected works. Those exemptions include those set forth in Sections 1201(e) ("information security" conducted under certain government contracts), 1201(g) ("encryption research") and 1201(j) ("security research"). The exemption serves to assure that security-based research, scholarship and criticism of the proposed classes of works that involves circumvention to demonstrate the security and privacy-related features, flaws and vulnerabilities is not treated as prohibited conduct, even where such research is not covered by another exception to 1201(a)(1)(A)'s general prohibition. This appears entirely consistent with the intent of Congress to promote robust testing and research in furtherance of secure computing and privacy.

The academic and business community has made substantial investments in improving the security and privacy associated with the use of digital works protected by copyright. Independent research firms, consultants and academic institutions regularly engage in the testing of properly licensed works in order to determine the existence of security-based features, flaws or vulnerabilities. This activity produces ongoing reports to the vendors and service providers associated with the works, to the users themselves and to the general public regarding the existence of such features, flaws or vulnerabilities. These reports help contribute to the adoption of continuing improvements that enhance the security of digital properties and services and improve the ability to protect the privacy of users against unexpected losses. Without the acceptance of the proposed exemption, much of this activity is likely to cease.

It is important to emphasize that the security-based research, scholarship and criticism otherwise prevented in the absence of the exemption is activity conducted by those with a lawful right of use regarding the protected works. No "hacking," "cracking" or unlawful attacks are intended to be authorized or permitted by the proposed exemption. Instead, by exempting the proposed class of works, authorized users can vigorously exercise their rights to assure themselves no unexpected features, flaws or vulnerabilities exist, or to identify, understand, and remediate or manage them if they do.

Related Harms

During 2002, more than 4000 reports concerning actual or potential security flaws in software that is used on computers, computer systems, and computer networks have been received by the CERT Coordination Center. This sampling does not include undisclosed reports made directly to software vendors or other organizations, nor does it include undiscovered or undetected features, flaws, or vulnerabilities. All of these reports should be subject to research in order to determine, for the benefit of users, the nature and extent of the risks they may introduce. Failure to do so will allow security risks that permit crimes, damage to systems, compromise of commercial and personal data, and otherwise harm to interests of legitimate users. In the absence of the proposed exemption, many of these security risks will not be properly researched and documented.

Additional specific data is available from the Computer Security Institute's "2002 Computer Crime and Security Survey." The Computer Security Institute conducts its annual survey with assistance from the FBI's Computer Intrusion Squad. Data from the 2002 survey includes:

- Ninety percent of respondents (primarily large corporations and government agencies) detected computer security breaches within the last twelve months.
- Eighty percent acknowledged financial losses due to computer breaches.
- Forty-four percent (223 respondents) were willing and/or able to quantify their financial losses. These 223 respondents reported $455,848,000 in financial losses.

- As in previous years, the most serious financial losses occurred through theft of proprietary information (26 respondents reported $170,827,000) and financial fraud (25 respondents reported $115,753,000).
- For the fifth year in a row, more respondents (74%) cited their Internet connection as a frequent point of attack than cited their internal systems as a frequent point of attack (33%).

With respect to many, if not most, of these losses, the intrusion or damage was made possible by the exploitation of a feature, flaw, or vulnerability within the proposed class of protected works.

Effects of the Proposed Exemption:

1. Effect on Availability

Unless the proposed exemption is granted, much of the software content (i.e. code) within the proposed class of works may be inaccessible to research of the security-related features, flows and vulnerabilities because of the use of technological access controls that prevent reviewing and testing software code.

2. Effect on Criticism, Comment, and News Reporting

The proposed exemption will have a positive effect on criticism, comment, and news reporting. The proposed exemption will ensure that threats of DMCA violations will not stand as a barrier to the evaluation of software security flaws.

3. Effect on Teaching, Research, and Scholarship

The proposed exemption will have a positive effect on teaching, research, and scholarship. The availability of independent research on existing software flaws directly aides and promotes teaching and scholarship by adding to the existing body of knowledge concerning software technology and products.

4. Effect on the Market

The proposed exemption will have a long-term beneficial effect on the market. Software quality is likely to be improved in an environment where flaws can freely be identified, discussed, and remediated. Awareness in the marketplace that products will be independently tested and flaws identified and remediated will tend to increase market confidence in such products.

5. Effect on Copyright Owners

The proposed exemption will have no effect on the rights of copyright holders. The proposal is limited to legally acquired protected works (including demonstration and trial versions).

Proposed Exemption #3

Compilations consisting of lists of websites blocked by filtering software applications -- The proposed exemption is fully supported by the rationale adopted by the Register in the initial exemption rulemaking under Section 1201(1)(a)(3). There have been no changes in the marketplace or in the related technologies or business practices that mitigate against the necessity for continuing the exemption

Proposed Exemption #4

Literary works, including computer programs and databases, protected by access control mechanisms that fail to permit access because of malfunction, damage or obsoleteness -- The proposed exemption is fully supported by the rationale adopted by the Register in the initial exemption rulemaking under Section 1201(1)(a)(3). There have been no changes in the marketplace or in the related technologies or business practices that mitigate against the necessity for continuing the exemption.