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 reply comment, supporting or amplifying comments submitted in the first comment period by Static Control Components, Inc., are submitted on behalf of CERT/CC.

Proposed Class(es) of Works

This reply comment is intended to support or amplify the earlier comments by Static Control Components, Inc., with respect to the following proposed classes of works:

1. Literary works including computer programs embedded in a machine or product and which cannot be copied during the ordinary operation or use of the machine or product.

2. Literary works including computer programs embedded in a machine or product and that control the operation of a machine or product connected thereto, but that do not otherwise control the performance, display or reproduction of copyrighted works that have an independent economic significance.

Summary of the Argument(s)

The following argument is offered in support of both of the proposed exemptions:

This comment in support of the proposed exemptions is made in order to relieve the restraints on security testing practices and vulnerability research for which the existing exception in Section 1201(j) is not adequate. The proposed exemptions should be granted in order to facilitate legitimate vulnerability testing of computer code embedded in devices. Access controls that prevent (a) legitimate research into the weaknesses of security measures used in computer code embedded in devices, and (b) the detection and amelioration of potentially destructive defects in embedded computer code, are likely to cause harm by allowing security flaws and potentially destructive defects in computer code to remain undetected. Such undetected security flaws, if not identified by legitimate vulnerability testing, are likely to be first discovered and exploited by individuals with malicious intent. Undetected vulnerabilities in embedded computer code, whether representing security weaknesses or operating defects, pose a particular risk of harm because they create a risk of damage to, or the loss of control over, the devices or infrastructure in which the code is embedded, potentially including components of critical national infrastructure systems.

With respect to computer code embedded in devices, vulnerability testing requires, in most cases, the circumvention of an access control because embedded code is generally not made readily accessible.

Argument in Support

Classes of Works

Literary works including computer programs embedded in a machine or product and which cannot be copied during the ordinary operation or use of the machine or product; Literary works including computer programs embedded in a machine or product and that control the operation of a machine or product connected thereto, but that do not otherwise control the performance, display or reproduction of copyrighted works that have an independent economic significance. While a broad range of machines, products, devices, and infrastructure contain embedded code, the balance of this comment will refer collectively to all such tangible assets as "devices."

Technological Controls

The technological controls used to control access to these categories of works vary. In many cases the application of embedded code is very narrow and the code is not readily accessible for any use or purpose other than the function the code serves. Thus, in order to conduct vulnerability testing on embedded code, in most instances, a researcher must circumvent some type of access control in order to access the code for analysis.

Prevented Activities

This category of works is defined by the types of non-infringing activities that it prevents, namely:

(a) legitimate research into latent security weaknesses in embedded computer code, and (b) the detection and amelioration of potentially destructive defects in embedded computer code.

Section 1201(j)(1) defines "security testing" to mean "accessing a computer, computer system, or computer network, solely for the purpose of good faith testing, investigating, or correcting, a security flaw or vulnerability, with the authorization of the owner or operator of such computer, computer system, or computer network." It does not appear that Section 1201(j) allows vulnerability testing on embedded code, because computer code embedded in devices, whether or not such code controls the operation of such devices, may not be included within the meaning of "computer, computer system, or computer network," the only subjects of security testing for which the exception is available. Accordingly, no existing exception to Section 1201(a)(1)(A) currently explicitly permits security research or vulnerability testing on embedded code.

If the current request for exemption is not considered favorably, the Register may wish to consider whether an exemption is appropriate to clarify that the scope of the exception under Section 1201(j) includes literary works in the form of computer code embedded into physical devices.

Related Harms

The inability to conduct research into security flaws or design defects results in such flaws and defects remaining undetected, increasing the likelihood that such flaws will be discovered and exploited by hackers and others with malicious or criminal intent. Preventing the discovery of such flaws by enforcing the anti-circumvention prohibition against legitimate researchers (who may not otherwise qualify for the exception available under Section 1201(g) or (j)) is likely to lead to otherwise preventable harm to the tangible devices and systems in which such code is embedded.

To the extent that access controls to embedded computer code prevent the detection and amelioration of potentially destructive defects in such code, researchers must have the ability to legally circumvent such access controls in order to prevent substantial potential harm to the devices and systems in which such code is embedded. Because of the increasing integration of computer code into devices, systems, and infrastructure, an ever-increasing proportion of tangible assets are placed at risk by security weaknesses or design defects in embedded code. The dangers posed by failing to detect and fix such security weaknesses or defects cannot be overstated. Critical infrastructure such as bridges, pipelines, dams, and water supply systems increasingly contain embedded code essential for their operation. Medical devices increasingly contain such code. It is not difficult to imagine the harm that could result from a security weakness in such a device being exploited by a malicious actor.

Legitimate research and testing on computer code embedded in devices does not appear to have been contemplated by Section 1201. Yet, the increasing prevalence of such code, and the increasing reliance of an incredibly broad array of tangible assets on such code, create an urgent need for robust research and testing to discover vulnerabilities that may threaten the assets themselves.

Effects of the Proposed Exemption

1. Effect on Availability

The proposed exemptions will have no effect on the availability of these classes of works. Because the proposed exemptions are limited to embedded computer code that cannot be copied and/or that has no independent use or marketable value, allowing circumvention of access controls to such works in order to facilitate vulnerability research will not result in any diminution in the market for the works. Indeed, such research may increase the market for such works by rendering them more reliable and increasing market confidence in their security and dependability.

2. 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 security flaws and design defects in embedded code benefits teaching and scholarship by adding to the existing body of knowledge concerning embedded software technology and its effects on the devices in which it is employed. Indeed, because research on embedded code almost always requires circumventing some type of access control in order to access such code, it is difficult to see how, under the current structure of the DMCA and without the proposed exemptions, any such research or scholarship may proceed in the United States to realize its full potential.

3. Effect on the Market

The proposed exemption will have a long-term beneficial effect on the market. The use of embedded computer code to enhance or control the operation of devices is likely to be improved in an environment where security flaws and defects in such code can freely be identified, studied, and remediated. Awareness in the marketplace that products relying on embedded computer code will be independently tested and flaws identified and remediated will tend to increase market confidence in such products.

There is a potential negative effect on the market for specific products that are found to contain security weaknesses and design defects that are not capable of being remediated. However, the broader market for embedded computer code generally will be strengthened by robust research and testing on vulnerabilities in such code.

4. Effect on Copyright Owners

The proposed exemption will have no effect on the rights of copyright holders. The proposal is limited to legally acquired copies of the proposed classes of works, attached to tangible devices that have been lawfully acquired, or where access to such devices has been lawfully obtained.

5. Additional Considerations

The DMCA was adopted for the purpose of inhibiting piracy of copyrighted works. It was not intended to inhibit vulnerability testing of computer code enhancing or controlling the operation of devices. While the DMCA is a first step toward controlling piracy while facilitating legitimate security and vulnerability research, CERT has consistently proposed in its prior comments to expand the exemptions to the anti-circumvention rules in ways that would better ensure that such valuable research might continue unimpeded, consistent with the spirit and intent of the DMCA. Earlier comments submitted by CERT, did not address the impact of the commercial practice of embedding software in devices, this comment is meant to highlight CERT's belief that embedded computer code should not be excluded from any exemption granted to advance research and testing.

This comment is submitted without regard for the specific merits of the Lexmark vs. SCC case (in which CERT/CC has no direct interest). CERT's interest in the proposed exemptions relates to legitimate vulnerability research and testing.