Michael A. Rolenz
10 February 2003
"Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies"

Reply comments in support and amplification to Comment #14 of Michael A. Rolenz

2. Descriptive Name Class : Information collected by "Spyware" software that is encrypted or "Spyware" software whose operation uses encryption to hide its operation

Summary:

The comment pertained to so called "spyware" which is functionally equivalent to a Trojan Horse computer virus program. In my previous submittal, I gave a brief history of spyware, descriptions of several widely distributed spyware programs, and their actions. Since that time, I have become aware of another class of spyware programs that uses electronic greeting cards as the means of delivering this spyware. This particular class would be especially useful for industrial or military espionage. I would like to add that as supporting evidence for my previous submittal.

Facts and evidence:

This new class of spyware has fused the characteristics of INTERNET "spammers" and computer viruses. Namely, this spyware uses electronic greeting cards to deliver the what for a computer virus would be called a "root kit"[1]. The pioneers in this area are a Canadian based pornography company called Cytron Communications Limited. Cytron specializes in using spammed email of electronic greetings with fake return addresses (e-greetings at yahoo.com). Clicking on the icon sends one to suprisecard.net where one must download software to read the greeting. The software is a Trojan Horse that installs a Browser Helper object into Microsoft Internet Explorer. This "helper" collects keywords from web pages that are browsed to identify "potential customers" for target advertisements of pornography on their webbrowser. Cytron in effect hijacks the unwitting recipients webbrowser and turns it into an pornography advertising machine.

Other spyware such as Email P.I. are even more insidious. The makers of this program market it as a way to check on "your cheating spouse". The email "I love you" message installs software that records email, chatrooms, passwords, webcams, keystrokes, websites visited, files downloaded, and documents accessed. The software is marketed to catch "cheating spouses" but clearly the true market is espionage-industrial, economic, and military[2].

Argument:

[1] So called because it installs itself into the main operating system directory or "root" folder in Unix and "hijacks" system functions.
[2] See http://www.infosecnews.com/opinion/2003/01/15_01.htm

The spyware described here and in the previous comment is functionally identical to the more virulent of the computer virus software that is well reported on news broadcasts. It uses the same techniques. Trojan horse programs are used to install surreptitious software that allows a remote user to capture all activity, take control of the computer. I truly wonder if one were to view the source code of several spyware programs one might not see actual sections of computer virus code that formerly were designed to trash a computer commented out[3] and replaced with sections that have the spyware reporting its findings to its remote control. Functionally there is no difference and spyware of this type is simply the commercialization of what has been an underground and often illegal activity.

As pointed out in the previous comment, spyware is problematical because as software it is copyrighted and so is the e-greetings used to deliver it. Under the DMCA, any access controls and encryption used to hide the operations[4] would be protected from circumvention. Circumvention is required not only to determine if suspected software is spyware, to study its workings, and ultimately to create the programs needed to remove it. While functionally, most spyware is equivalent to computer viruses, the commercial vendors of anti-virus software have not addressed the issue of spyware. The work that has been done has primarily been by a small community of people without the financial resources to bear the costs of protracted litigation[5].

While computer viruses existed for nearly two decades and have become quite sophisticated, spyware is a relatively recent invention. Already, spyware programs have adapted the technology and methods of computer viruses very successfully already. Given the protection of the DMCA, they are sure to flourish in the future. For these reasons I urge the Librarian of Congress to grant an exemption for the study of spyware programs and the unfettered dissemination of the results of that study.

---

[3] Computer languages allow programmers to put in non executable statements into their code called comments. The purpose is to let the programmer put in notes in the code or to format it to make it easier to read. Programmers often use the comment feature to prevent statement from being executed by converting them to comments in the source listing.

[4] I have not been able to determine if Email PI uses encryption or what their access controls are but as shown in my previous submittal, even Barbie software has the capability and does use it.

[5] The argument can be made that since spyware is functionally identical to computer virus, that spyware should be covered by the same sorts of laws covering computer viruses. The fundamental problem there is that unlike a computer virus, the effect of spyware is not as “dramatic”. Its nature only becomes evident after suspicion and study which requires circumvention.