From: Glenn C. Everhart
Everhart@gce.com
156 Clark Farm Rd., Smyrna, Del. 19977 302 659 0460

The Millennium Copyright Act: Aid to Crime?

MCA is in danger of being interpreted to legally sanction a vast range of criminal, tortious, or fraudulent activity.

Distinguishing authorized computer access from unauth depends on telling when a subject is permitted to access an object. This becomes very hard where scripts are involved, mitigated by ability to read the scripts. Where programs are involved, the checking needed to determine whether harmful or unwanted activity is going on is much harder and needs tools able to inspect what the programs are doing.

Most current computer virii and breakins use program internal scripts and other actions which are hidden from users. These hidden actions are therefore precisely what computer security workers must be able to inspect.

It is vital that no legal barriers to performing this inspection in the service of lawful purposes be erected. The creation of hidden (covert) behavior in programs to prevent unlicensed use must not be allowed to become a cover for restrictions which have nothing to do with theft of content but may be imposed to invade privacy, destabilize competing software, reveal private information, or control which other software may be used at a customer premises.

I work in information security at a bank, a large credit card issuer. We deal constantly with threats from software malfunctions and holes which could cause customer information (that means your account information, personal data, card numbers, and so on) to be released. To prevent this we must inspect software and media, must be able to check what programs do and what data may contain (it is possible to hide quite a lot of customer information inside movies or sound files; this can be checked for so long as the movies or sound files are not encrypted), and must be able to do our looking preferably on platforms where the software is unlikely to contain secret functionality we have not known.

We have not the time or manpower to write all our own cryptanalysis software but use commercial and freely available programs for this purpose. To keep inappropriate content out of the bank, and to keep customer data (or other confidential information) from going out, we must inspect media. We prefer to be able to inspect on platforms such as secured unix boxes rather than windows, because they have less unadvertised behavior and we can monitor what they do closely. That is hard on windows. The availability of CSS descrambling allows examination of DVD information for stegonography (which would hide information). We need to be able to do that, and will need to be able to do so more in the future.

The DeCSS controversy is an example of fake issues being raised by the MPAA here. The CSS system was advertised as copy protection. It is no

such thing, since the ciphertext can be copied and played the same as the original, with no loss of fidelity and no control of the number of such copies that may be made. Rather, their actions are directed to keeping DVD from being analyzable for hidden content and to keeping them from being used compatibly with operating systems other than Windows. (Reasons for this are alleged to have to do with non-US use, which has nothing to do with a US law.) They aim at creating a form of encryption which it is forbidden to break, leaving a gigantic hole for use in the service of criminal fraud to use in moving financial data.

You can't run a bank security system without checking media that go in and out for financial data. We're going to have these media coming in and out, and must have access to tools to let us check it for concealed information. (Remember: the personal information that may be stolen could be yours.)

The more general issue of hidden functions is a concern too. We have seen many instances of software with hidden functions that sabotage competing software (which vendors call "bugs" when they get caught at it). We have seen too many cases where programs capture and send out user information to vendors with no notice to those whose information is being stolen. Part of our department's responsibility is to find some of these cases and keep the information from being sent out of the bank. We need the tools to keep our systems working, and cannot live with laws or regulations which say, in effect, "you're interfering with an access control system and cannot get or send information about how to let your programs work with one another".

May I plead that the MCA be interpreted so that access control is understood as dealing narrowly with schemes which keep digital content from being used where not paid for. Let the rules be clear that where content is paid for, it may be used according to normal commercial rules, and any tools that facilitate such lawful use and lawful testing for safety are also legal.

If (for the specific DVD case) I buy a DVD with a movie on it, I should be able to watch it on any computer I have with a drive, on any DVD player I have, and I should be able to check it for hidden contents if I need to. (I should not be spreading duplicates, but the CSS system does nothing about this; the size of the media makes duplicating DVD impractical, but CSS does nothing to prevent copying, nor does CSS descrambling encourage duplication since the DVD can be duplicated without decryption and the copy used.)

If I buy a piece of software I should be able to run it as I would have expected. I should not have to put up with the software system insisting on sending information about my computer to someone else, much less sending any other information about my web viewing habits, what else I have on the box, my personal data or the like, somewhere I am not told about. It is reasonable to say I shouldn't be spreading a tool that disables the software from requiring a serial number, for example. It is not reasonable that I should be prohibited from sending out a tool that blocks the software from massively invading my privacy or that of others.

Sending out information without authorization by the computer owner

is a form of theft: theft of information, and theft of service on the computer. Sabotage, whether intentional or accidental, is also a form of theft. It is contrary to the whole tenor of the legal system to claim that a law now protects these forms of theft (and possibly many more) by allowing people to claim they are part of access control systems.

The rules need to pierce this curtain and make it clear that access control is limited in scope to what controls access within the bounds of the access which is normally expected for content. They should not work to extend the control of a seller far beyond what it has ever been and enable the growth of a vast amount of basically criminal function under the guise of access control.