Overview of CRA and Felten et al.

Ed Lazowska
July 1, 2001
Updated August 9, 2001

Background on Felten et al.

In September 2000, SDMI announced a "public challenge" in which it invited members of the public to try to break certain data-encoding technologies (4 watermarking technologies and 2 other security technologies) that SDMI had developed. No documentation explained the implementations of the technologies, and no watermark embedding or detecting software was directly accessible to challenge participants. Felten et al. accepted the challenge, and described their results in the research paper *Reading Between the Lines: Lessons from the SDMI Challenge*. This paper was submitted to, and accepted by, the Fourth International Information Hiding Workshop in late April, but Felten et al. eventually declined to present the paper and withdrew it from the conference due to DMCA-based intimidation by RIAA, the SDMI Foundation, and the Verance Corporation. Background materials, including a preliminary draft of the paper itself (not authorized by the authors), are available at http://cryptome.org/sdmi-attack.htm.

Felten et al. subsequently submitted the paper to the 10th USENIX Security Symposium in August. EFF, representing Felten et al. and the USENIX Association, filed a complaint for declaratory judgment and injunctive relief to allow presentation of the research. The EFF complaint is available at http://www.eff.org/sc/felten/20010606_eff_complaint.html. The Computing Research Association determined to file an amicus brief in this matter.

RIAA, SDMI, and Verance subsequently stated in writing that they would not sue over presentation of the current paper, and filed a motion to dismiss the current EFF case. EFF opposed this motion, asserting that additional related research is in the pipeline, and that even if it were not, a Constitutional challenge should be allowed to go forward because the chilling effect of DMCA on free speech has already been demonstrated. CRA determined to file a declaration in this matter.

Background on CRA

The Computing Research Association is a nonprofit organization headquartered in Washington, DC. CRA counts among its members some 200 North American organizations active in computing research. These include academic departments and academic, industrial, and government laboratories. CRA works with these organizations to represent the computing research community and to effect change that benefits both computing research and society.

CRA seeks to strengthen research and advanced education in computing and allied fields. It works to influence policy that affects computing research, encourages the development of human resources, and contributes to the cohesiveness of the professional community. Collecting and disseminating information about the importance and state of computing research play important roles in achieving these objectives.

Supporting a vibrant computing research community is CRA's mission. DMCA, as used by RIAA, SDMI, and Verance, poses a direct threat to the computing research enterprise.

Further information on CRA is available at http://www.cra.org.

The nature of research in general, and of computer systems research in particular

Much research in computer system is based upon *analysis* – the careful examination of existing systems and approaches, in order to understand what works well and what works badly. This sort of examination leads to improvements that are both evolutionary and revolutionary. You discover flaws. You invent new and/or improved ways to detect flaws. You invent new and/or improved approaches to system design and implementation. This investigative approach has driven the computer systems field forward for more than half a century.

Open publication of research results is essential to the conduct of research. The computing research community is large – many thousands of individuals. It is ever-expanding: students join the research community, providing continual refreshment, and mature researchers move from one subfield to another, in each case by studying the literature. All of computer science, and indeed all of science, is increasingly inter-dependent – results in one field or subfield are relevant to researchers in other fields or subfields. Broad review and critique are fundamental to the advancement of research. Closed communities do not make progress at nearly the rate of open communities.

There is a long history of open research in computer security and information hiding. This is obvious simply from the fact that the Felten et al. paper was submitted to the *Fourth* International Information Hiding Workshop and then to the *10th* USENIX Security Symposium. Most of the security and information hiding technologies upon which we rely today are the products of this research process.

The Felten et al. paper provides a useful case study of this research process, and of the benefits of open publication:

- For those who do research in copy protection and/or information hiding, the paper provides a careful scientific case study of 6 approaches, using a variety of analytic techniques. The paper makes specific contributions to deepening our understanding of why watermarking based upon echo hiding is not a viable technique – a fact first exposed in a paper published two years earlier by others. The paper exposes the hurdles that future watermarking techniques must overcome if they are to be successful. The paper has *already* led to significantly improved approaches to watermarking.

- For those who are peripherally interested in copy protection and/or information hiding – for example, potential users rather than researchers – the paper demonstrates that the approaches advocated by RIAA, SDMI, and Verance *will not provide protection*. If you are, for example, a recording studio or a recording artist, *this matters to you*. Verance still insists that their technology is practical and secure – their business depends upon the continued sale and use of this technology! *Of course, Verance does not want the Felten et al. results published!*

The DMCA

The problematical portion of the DMCA is *Sec. 1201 Circumvention of copyright protection systems,* specifically:

> *(2) No person shall manufacture, import, offer to the public, provide, or otherwise traffic in any technology, product, service, device, component, or part thereof, that –*
>
> *(A) is primarily designed or produced for the purpose of circumventing a technological measure that effectively controls access to a work protected under this title;*
>
> *(B) has only limited commercially significant purpose or use other than to circumvent a technological measure that effectively controls access to a work protected under this title; or*
>
> *(C) is marketed by that person or another acting in concert with that person with that person's knowledge for use in circumventing a technological measure that effectively controls access to a work protected under this title.*

We would assert that this text is both *ambiguous*, and *unnecessarily overly broad* (going far beyond what the Congress had in mind, namely to strengthen copyright).

The word "technology" in (2) is ambiguous. For example, RIAA represents that Felten et al.'s research paper is "technology" under the Act.

The word "part" in (2) is extremely broad. I spoke above of the "connectedness" of much of computer science, and science as a whole. Many researchers build analysis tools – low-level debugging and/or tracing tools, dual-booting techniques, interoperability techniques. These analysis tools have broad applicability, including copy protection and/or information hiding research. Will all analysis tools be interpreted as being in violation of the DMCA because they can potentially be of value in research related to copy protection and/or information hiding? DMCA prohibitions reach back into other fields that feed forward into security fields.

The phrase "commercially significant purpose" in (B) can be used to exclude research (which may not have an obvious commercial value).