

Current Events

PGP

Phil Zimmerman's Pretty Good Privacy encryption software is no longer being supported by Network Associates, Inc., the company that owns the trademark rights according to an article in yesterday's Daily Camera.

"Network Associates, which bought PGP from Zimmermann's PGP Inc. in 1997, sought a buyer last year for its e-mail and file encryption products. The company said it didn't get an attractive offer, so it dropped the products earlier this year.

Though some longtime PGP users insist Network Associates could have marketed the product better, others say the demand simply wasn't there.

PGP

“People aren’t spending for encrypted e-mail,” said Austin Hill chief strategy officer at Zero-Knowledge Systems Inc.

He ought to know. His company dropped plans for PGP as well.

Encryption is difficult for average users to grasp, products aren’t all that easy to use and the threats of not protecting e-mail from prying eyes aren’t all that easy to explain, Hill said.

Internet users won’t worry about using regular e-mail for credit card numbers, medical discussions and other sensitive information until they are directly harmed or see a well-publicized breach, security experts say.

Only then would they understand or care that using unencrypted e-mail is as private as sending a postcard. Without encryption, network administrators at Internet service providers, employers, intelligence agencies and hackers can snoop on email in transit.

PGP

“Many people believe that PGP from (Network Associates) was the only thing that existed,” said Fabian Rodriguez, associate director of business development at Toxik Technologies Inc., a PGP vendor. “Now that it’s not there, it sets the groundlevel equal for everybody.”

PGP alternatives include the Gnu Privacy Guard, developed by volunteers under a license that permits anyone to freely use, modify and further distribute the product.

Lok Technology Inc. offers Web-based e-mail accounts that use PGP, while Authora Inc. makes PGP work with Outlook e-mail software and any Web-based e-mail system. Toxik handles data sent through online forms.

PGP

Other-encryption methods exist, but none has PGP's popularity.

The alternatives still need work.

Authora, for instance, lacks compatibility with non-Microsoft e-mail software such as Eudora and Lotus Notes.

Gnu is only a command-line program and needs a graphical interface to be attractive to the vast majority of users. A few interfaces, including Windows Privacy Tray, have been developed but none are as versatile or simple as Network Associates' program.

PGP

Phil Zimmerman's comments:

"PGP has been around for 10 years, and has endured incredible obstacles and hardships," Zimmermann said. "Powerful forces have been arrayed to stop PGP and yet those obstacles were overcome."

"People are very concerned about this development and would like to do something about it," Zimmermann said. "A way will be found."

The HDCP Crack

High-bandwidth Digital Content Protection, or HDCP, is intended to secure communication over the interface that now connects a computer or set-top box to a display or television, ensuring that the signal is never exposed as plaintext.

In this scheme, each manufacturer purchases a license from an authority that includes, for each device X , a key exchange vector v_X and a private vector u_X in the module $M \subset (\mathbb{Z}/2^{56} \mathbb{Z})^{40}$. When devices A and B want to communicate, they exchange their key exchange vectors, and device A computes the dot product $u_A \cdot v_B$ and device B the dot product $u_B \cdot v_A$. The authority uses secret information to choose the keys, ensuring that for any pair of devices the two dot products will have the same value.

The HDCP Crack

David Wagner working with Ian Goldberg, Scott Crosby of Carnegie Mellon University, and two students, showed that to know the secret, it suffices for an attacker to obtain 40 public/private key pairs, such that the public keys span the module generated by all the public keys. Since HDCP devices readily divulge their public keys, this is an easy task.

Once the secret is known to the attacker, the entire scheme is wide open. The attacker can intercept encrypted communications, spoof trusted systems, or even manufacture his own HDCP devices without a license, It's exactly such a situation — a commercial disaster for companies relying on the technology — that the DMCA was intended to prevent.—SR

Source: *SIAM News*, Jan/Feb 2002 by Sara Robinson

DMCA

Wagner, a professor of computer science at the University of California, Berkeley, has a long-standing interest in the security of commercial systems. As graduate students, he and his colleague Ian Goldberg were featured in The New York Times, first (1995) for cracking an early version of Netscape's Secure Socket Layer, a system that encrypts financial transactions over the Internet, and later (1999) for showing how to clone cell phones of a type widely used in Europe.

After the SSL crack, even though it had to rush to release a new version of its software, Netscape showered Wagner and Goldberg with free t-shirts and other expressions of gratitude. If Wagner and Goldberg hadn't found the flaw, someone else, perhaps with less honorable intentions, surely would have done so.

DMCA

With the recent HDCP result, however Wagner published his research only after several months of consultation with university lawyers. In the era of the Digital Millennium Copyright Act (DMCA), enacted in 1998, publishing such research could subject him to heavy fines or even several years in prison. In the future, Wagner says, he plans to stay away at least from copy-protection research, because it has “too much overhead.”

Wagner’s concerns are with the part of the DMCA known as the “anti-circumvention” provision, one piece of which makes it illegal to circumvent technological measures that control access to or prevent copying of copyrighted material. Another piece makes it illegal to create or distribute tools that enable the circumvention of such measures.

DMCA

The law does specify some exceptions to the rule: Engineers are allowed to reverse-engineer software for the purpose of achieving compatibility with other products, for instance, and academic computer security researchers, like Wagner, are allowed to crack encryption protocols for research purposes.

Still, while the law permits the research, it's not at all clear whether researchers can legally create or disseminate software verifying that their security-cracking algorithms work. It's also not clear whether publishing an academic paper, or giving a talk at a conference, is equivalent, legally speaking, to disseminating tools. Representatives from the entertainment industry have taken the position that such activities are illegal under the DMCA. In theory, the law could apply to anyone who demonstrates how to break a general-purpose encryption algorithm, such as RSA, if that algorithm has been used by some company to protect its copyrighted material.

Until the legal boundaries of the DMCA are further clarified by the courts, many researchers are proceeding cautiously. What he finds most risky, Wagner says, is “doing work that embarrasses someone.”

DCMA

So far, the courts seem more sympathetic to the piracy concerns of the record and movie companies than to the need of academics for unfettered research programs. In three ongoing DMCA-related cases, the decisions have been in favor of the entertainment industry. If academics want to defend their rights, they need to do a better job of conveying the importance of what they do and the harm caused by the DMCA's restrictions.

Professor goes to court

It's hard to believe that an academic could be prosecuted for the content of his research, but it almost happened to Edward Felten, a professor of computer science at Princeton University. Working with researchers from Rice University and Xerox PARC, Felten had participated in a recording industry-sponsored challenge intended to test the security of several schemes, mostly watermarking systems, for protecting digital music. The recording industry was offering a \$10,000 prize to anyone who could crack all the schemes within a certain time frame, given limited information about them. To be eligible for the prize, participants had to sign a non-disclosure agreement; Felten's group chose not to sign.

After his group had cracked four of the six schemes (all that was possible, he said, with the limited information given), Felten and his colleagues wrote up their results and submitted them to a computer security conference. When an executive from one of the companies developing the watermarks asked for a copy, Felten was happy to oblige; the executive and the Recording Industry Association of America then asked him to omit some details from the paper.

Professor goes to court

Felten, after consulting with his co-authors, decided that the details were necessary to support the conclusions and declined. This prompted letters asserting that speaking or writing about the challenge could constitute a violation of the DMCA. Not wanting to go through litigation, Felten's group chose to withdraw their paper from the conference. Meanwhile, a group of French researchers, not subject to U.S. copy-right laws, published their own crack of the schemes on their Web site. Later, with the support of the Electronic Frontier Foundation, a civil liberties group, Felten filed a suit of his own, asking the court for a declaratory judgment stating that he and his colleagues were free to publish their work in any form. Wagner and several other prominent computer scientists signed on to an amicus brief in Felten's support.

By that time, however, the recording industry lawyer, perhaps realizing that the case could establish an unfavorable precedent, had backed off, claiming that the intention had never been to sue Felten. Still, the EFF pressed forward, saying that the threat of lawsuits was having a chilling effect on research. In December, however, a judge ruled that there was no conflict and dismissed the case.

Another Case

In another decision, a federal appeals court upheld the ruling of a lower court against Eric Corley, publisher of a Web site devoted to news for hackers. Corley was sued by the movie industry after he published a copy of a program called DeCSS, written by a young Norwegian hacker, that breaks the copy and access controls for DVDs. The EFF funded Corley's defense, arguing that in publishing and linking to the program he was exercising his First Amendment rights. Still, a district judge enjoined Corley from posting or even linking to the program, ruling that the dangers posed by the functional aspects of the program outweighed Corley's right to free expression.

Elcomsoft

A third decision, in the first case of criminal prosecution under the DMCA, allowed Dmitry Sklyarov, a programmer employed by the Russian company Elcomsoft, to walk free as long as he agreed to testify against his employer. Sklyarov was arrested by FBI agents after he spoke at a hacker conference in Las Vegas because, while working for his employer, he had written a program that circumvented the copy and access controls for Adobe eBooks. Such programs are legal in Russia; however, Elcomsoft ran up against the DMCA because it was selling the program on the Internet via a Seattle-based company. The FBI continues to pursue its case against Elcomsoft.

Industry Perspective

To many scientists, DMCA-style intellectual property protection seems to come at such a high cost that it's hard to see why anyone would support it. But the law does have, significant support, and not only from entertainment executives. Among its proponents are artists, business executives, and, seemingly, some judges and lawmakers. This group sees the research restrictions as a necessary evil for protecting intellectual property in the digital age, just as the law's opponents see difficulty in enforcing intellectual property rights as a necessary evil for protecting freedom of expression.

Creation of the DMCA was prompted by concerns that new technologies had the potential to make old copyright laws unenforceable. The old laws focused on the act of copyright infringement, rather than on the production of tools that make infringement possible. While it was legal to manufacture and sell printing presses or copy machines, it was illegal to make and sell a thousand copies of a book you had bought.

Industry Perspective

This approach to protecting intellectual property was effective because of the high overhead costs of making and distributing large numbers of good-quality copies. It was easy to focus enforcement efforts on large-scale infringement operations, and the hardcore crooks behind them.

With digital technology, however, any individual with a personal computer can make large numbers of perfect copies of a document, a song, or a film. These copies can be widely disseminated via e-mail, newsgroups, or file-sharing programs.

Security schemes can slow the dissemination process, but no practical security system could provide foolproof protection against infringement. In such a world, the entertainment companies have argued, just going after the infringers is no longer a sufficient strategy. Entertainment companies say they cannot keep tabs on individual PC users, but they can go after distributors of software.

Industry Perspective

Mark D. Litvack, vice president and legal director of antipiracy at the Motion Picture Association of America, compares the DMCA to laws that prohibit passengers from carrying weapons on planes: “Carrying a pocket knife on a plane, in and of itself, doesn’t damage anything,” he says. “But we arrest people who do it because the potential for harm is so bad, we want to stop the action before the harm occurs.”

DMCA opponents might reply that Litvack’s method is akin to prosecuting knife manufacturers. Still, the concerns raised by the entertainment companies are real ones. Technology is indeed a threat to traditional means of enforcing intellectual property rights, and academics need to present a better alternative to the DMCA than the overthrow of the entertainment industry’s business model.

The Opposition

Not surprisingly, the law has prompted a popular outcry, but mainly from groups whose members, like computer security researchers, seem to hold themselves apart from the pragmatic rules governing the business world. The hacker community, for instance, has been the law's most consistently vocal opponent. In some sense, the DMCA is an attempt to do away with the general-purpose von Neumann computer and replace it with computers that allow only certain types of programs and operations. To a hacker, a computer is like a musical instrument in that its use should be limited only by the skill of its operator. In much of the business world, where "hacker" is synonymous with someone who breaks into computer networks, this point of view doesn't garner much sympathy.

The rest of the opposition consists of civil liberties groups like the Electronic Frontier Foundation, whose members are often viewed in the business world as fringe elements akin to animal rights activists, and perhaps the most persuasive of the anti-DMCA activists: academic intellectual property attorneys.

The Opposition

Academic intellectual property attorneys have rallied against the DMCA because of concerns that the law upsets a careful balance that copyright law aims to achieve. As American University law professor Peter Jaszi points out, the monopoly given by copyright law to the copyright holders was carefully balanced by other principles, such as fair use.

Under the DMCA, entertainment companies can not only prevent you from making copies of digital books and music, they can dictate how you use them. This gives the copyright holder too much power at the expense of the rights of the individual, Jaszi says.

For researchers, however, concerns about the DMCA center primarily around the right to perform and publish research freely—certainly a First Amendment issue, but also a practical one. And it's the practical issue that has the greatest potential to sway Congress and the courts.

What is next?

Part of the problem for the entertainment companies is that manufacturers of consumer electronics don't want to implement good encryption in their products; such schemes are expensive and would force them to raise their prices. With HDCP, for instance, Intel programmers told Wagner that they chose not to use RSA, or similarly well-tested schemes, because of the manufacturers' limits on the number of computational gates they were willing to implement. The world promoted by the entertainment companies, then, is one in which the security systems for intellectual property will offer mainly legal, and very little technical, protection.

The problem with this approach is that it's impossible to separate security technology for intellectual property from general security technology. Promoting the spread of such systems while suppressing efforts to design more secure systems could jeopardize other products, such as firewalls, general-purpose encryption software, and authentication schemes.

If researchers can raise public awareness of this threat, along with viable alternatives to the DMCA's approach to intellectual property protection, Congress and the courts might reshape the DMCA into something less harmful.

Reference

This article is:

Awaiting DMCA Clarification, Researchers Proceed Cautiously

in SIAM News, Jan/Feb 2002. Written by Sara Robinson.

Sara Robinson is a freelance writer and part-time journalist-in-residence at the Mathematical Sciences Research Institute in Berkeley.