Putting a Trace on Copyrighted Booty

Paul Kocher's technology would allow investigators to track pirated material's provenance -- without snooping on the innocent

Star cryptographer Paul Kocher's business strategy is simple: Search out industries that are losing money because of security holes and then find ways to plug them. So it's no surprise that Kocher has zeroed in on Hollywood, which views global piracy of movies with dread. The illicit swapping of music files online has already ravaged the music industry, which saw CD shipments fall 9% in 2002, according to industry trade group the Recording Industry Association of America (RIAA). Movie piracy is already big business -- and it only threatens to get worse.

Kocher's approach to taming piracy, however, is vastly different -- and less privacy-invasive -- than the proposed solutions from technology giants such as Microsoft (MSFT) or the legislative solutions being sought on Capitol Hill. Instead of trying to track everyone's habits and patterns, Kocher's code would create a forensic trail to allow law-enforcement authorities to hunt down criminals -- but only after there is evidence that illegal copies have been made. Says Kocher: "We're trying to create a system where there will be consequences if people don't obey the laws, but anonymity will be protected if they do."

Though Kocher's work is still in the research stage, his ideas are getting rave reviews from Hollywood studios, as well as DVD-player manufacturers. Small wonder. Whiz kid Kocher, 29, is the creator of Secure Socket Layer (SSL), a security protocol that allows Internet users to make secure online purchases. His eight-person company, San Francisco-based Cryptography Research, serves multinational clients, including Netscape, Microsoft, Visa Intl., and Mondex, MasterCard's smart-card division.

Kocher stresses that it isn't necessary to trade privacy for security: "The people that attack credit-card networks, that commit piracy, that commit identity theft -- it's the same people. And you've got to keep them from dominating. But, at the same time, you don't want to punish the legitimate guy."

On May 15, I sat down with Kocher in New York to discuss his approach to battling piracy. Following are edited excerpts of our conversation:

Q: Protecting intellectual property and copyrighted works is tricky. What's your solution?  
A: We've been trying to come up with a compromise. We've figured a way that, rather than reporting what customers are doing over phone lines or cable pipes -- which is really a serious problem from a privacy perspective -- we put any information you want to carry actually into the content itself.

If somebody makes a copy of a complete work, you can trace that back to the device that was used. But if you're not making a copy, or if you're making copies and only using them within your house or even giving them to a friend who doesn't distribute them, then there's no record of what happens.
Q: That makes sense. Why hasn't someone done it before?  
A: Technologically, this is really quite difficult to do. Right now, in a normal security device -- like a DVD player -- there's some code that sits in the player that decrypts data using keys that are "baked" into the player.

In order to get a technique like mine to work, what you actually have to do is make it so that, instead of decrypting the disk the same way in every player, each player decrypts in its own unique way. That way, when illegal copies are found, they can be traced back to the specific disk and machine from which they were made.

In fact, you have to actually go beyond that, because your bad guy or bad people may take multiple players, for example, and compare the output and try to eradicate the differences, so that law enforcement can't then figure out which devices were used. So you need to build the key management using some fairly sophisticated techniques. And that means putting a lot of that logic on as program code with the content.

Q: What does this mean to the consumer?  
A: From a customer perspective, it would be the same. You drop a disk in your DVD player and hit "play." But what actually ends up happening is a little bit of code from that disk works with information stored on the player and, together, they control the decryption process.

Q: How does this help prevent copyright infringement and protect privacy?  
A: The approach doesn't prevent anything. But it lets an investigator, who has already got proof that there was a crime, go through and trace it back to the device. We call it forensic marketing.

My research group believes it's the most customer-friendly thing you can do. Unless you're breaking the rules, you get your anonymity. But when you start breaking the rules, then it's easy to see who's doing what.

Q: How are entertainment companies responding to the idea? Until now, many studios have tried to foist the responsibility of copy protection onto technology companies.  
A: We're getting a very warm reception from Hollywood studios. And that's good. My philosophy on this -- which is kind of reflected in the research we're doing -- is that Hollywood takes the risk and it's their problem. To a large extent, they should bear the costs of developing countermeasures against attacks.

There are two reasons why I think Hollywood should be paying for it. One is that it's their content, so they'll make the most rational choices about how much to spend on security. Two, from a financial perspective, the consumer-electronic device makers have no incentive to do it right. Their job is to produce boxes that customers want to buy and not to go around solving somebody else's problem.

Q: Is this a model that exists in other industries?  
A: Yeah. The direction we're coming from here is, in a large part, motivated by work we've done for credit-card companies. If your card is stolen and used for fraudulent purposes, theoretically you can lose $50 out of it, but really, it's nothing. You don't have any liability as a customer. It's up to the banks to control fraud because they take the hit. And they do a pretty good job.

They'll never get rid of it, but fraud rates for the credit-card networks are around 0.07%. And if
Hollywood could have their piracy rates be 0.07%, they would probably be delighted. That's vastly better than what anybody would expect to achieve.

**Q:** So when will we see products that embed your ideal security?

**A:** This is still very much in the research phase. It's not going to pop up in any products next month.

Black covers privacy issues for BusinessWeek Online in her twice-monthly Privacy Matters column

Edited by Patricia O'Connell