Education
Editors: Matt Bishop, bishop@cs.ucdavis.edu
Deborah A. Frincke, deborah.frincke@pnl.gov

Who Owns Your Computer?

Matt Bishop
University of California, Davis

Deborah A. Frincke
Pacific Northwest National Laboratory

"Education, properly understood, is that which teaches discernment."
—*Joseph Roux*

Sony's much-debated choice to use rootkit-like technology to protect intellectual property highlights the increasingly blurry line between who can, should, or does control interactions among computational devices, algorithms embodied in software, and data upon which they act.

In November 2005, Sony BMG Music Entertainment issued a recall involving more than 2.1 million CDs sold with XCP, the copy-protection software developed in England by First4Internet. To play the CDs on a PC, users had to install a proprietary music player. As part of the installation, the XCP software modified the kernel to prevent illegal copying of the music. The modifications concealed themselves from the computer owner using techniques that rootkits use. The result was eloquently summarized in *IEEE Spectrum*: "Sony BMG shoots itself—and its customers—in the foot."[1]

The debate arises, in part, from the fact that XCP introduced a vulnerability that hackers exploited within a few days of its release.[2] The use of attack technology fueled the debate, as did certain statements from Sony executives. For example, Thomas Hesse, president of Sony BMG's global digital business, quipped that "most people don't even know what a rootkit is, so why should they care about it?"[3] However, consumers' understanding of technical issues regarding rootkits and operating system kernels, and how they affect decisions about managing technology, isn't the point of this article. Instead, our focus is on issues of security policy and appropriate defense. With respect to policy and defense, two key questions emerge:

- When systems or computational elements are combined, whose policy and expectation dominates?
- What sorts of defenses are appropriate, and in which situations?

The challenge to educators is to provide the experiences, and seek the understanding, that let others make better choices when such conflicts arise in the future.

Yours, mine, and ours

Many consumers were unhappy that Sony's software modified the kernel in a way they felt was inappropriate. Others felt that a supposedly benign product with a passive function—to provide music for listening—shouldn't have modified their computers without consent, let alone camouflaged those changes. This violated their "policy" of controlling their systems, as well as their expectation that playing CDs shouldn't introduce vulnerabilities.

Consider the matter abstractly. The owner of a computer with an unmodified operating system can copy data from a proprietary CD, as some fraction of the population is likely to do, despite regulatory prohibitions. The intellectual-property owner can make CDs in a way that forces the consumer to install software to prevent the copying. This software modifies the consumer's computer to enforce a new policy that disallows copying the intellectual property or removing the enforcement software.

Examining Sony's actions, we can consider the conflict between the consumer's policy (disallowing unknown modifications to the kernel that add vulnerabilities) and the owner's policy (disallowing copying). Further, the conflict's resolution involved a specific mechanism designed to override mechanisms that were enforcing a different policy. This brings out the difference between policy and mechanism, which is a sticking point for many students.

Next, consider the general goal of protecting data from being read or altered "illicitly." This might mean keeping data, such as checkbook information, confidential; controlling access to data such as medical records or homework assignments; and maintaining the integrity of key system files and components, such as authentication information or, ultimately, the kernel.

Any system must maintain the operating system's integrity. If the kernel is violated, the system is vulnerable to attack and other security mechanisms can't rightfully trust its reliability and correctness. Linux kernel-loadable modules that implement rootkits exploit the trust in the kernel, and damage its integrity, so system calls return erroneous information. The kernel is critical to the system's correct operation.

The view of a system must include the environment in which it is used.

Yet, the view of a system must include the environment in which it is used. Security policies for small offices typically tolerate some system crashes with minimal harm. If the system goes down, administrators can reboot it. Now imagine applying a similar policy to a medical computer that feeds medication through an intravenous feeding tube. Any crash while such a system is in use endangers a patient's life.

Interestingly, many best practices and standards for security exhibit this common flaw, assuming a particular context or environment without explicitly stating it. A fun exercise is to present students a set of rules or best practices documents and ask them to construct two systems: the first follows all the rules but is obviously insecure, and the second breaks some rules while maintaining security.[4] This drives home security's dependence on both definition and environment.

When is a defense offensive?

Sony embedded defenses in its CDs that actively breached the defense mechanisms protecting computers' kernels. In this instance, the CD producer's policy dominated the CD purchaser's policy, forcing the consumer's computer to enforce the data owner's policy.

This embedding of security policy within data illustrates a core concept for modern technologists. As we increasingly call for integrating security into systems, we can easily brainstorm situations in which the data owner's policy should prevail over the preferences of the owner of the software processing it or the computer doing the work. Having data that can defend itself—in which security is built into the file system or media without relying on existing software or hardware for protection—is beneficial in many situations. Even in this instance, consider what might have been if the CD hadn't introduced a vulnerability or if the defense had been easily reversible (perhaps without allowing users to continue using the CD). Would public opinion have been different if consumers had known the full ramifications of installing these CDs and fully consented to it at the point of purchase? Would we be touting Sony's forward thinking?

The question of when particular forms of defense are acceptable is arising more and more often.[5] Should limits apply to a defense that a CD imposes to protect its data from being illicitly copied? Are proactive defenses acceptable? What about responsive defenses, in which mechanisms in the CD take action after the data is copied illicitly? This is clearly a matter for debate and research, in both the ivory tower and society as a whole.

Active defense is a difficult topic, and it inevitably turns to concerns about unintended consequences. One author's personal favorite example involves software filters that parents (and libraries) can use to ensure that children (or others) don't visit pornographic Web sites. The use of such filters is controversial, even when used only where children might be at risk for sexual predation (for example, when using computers unattended in schools, homes, and libraries). Filters typically use lists of sites known to be pornographic, as well as words that indicate pornography or other objectionable content. At one point, however, filters blocked access to the White House Web site because a Web page contained the word "couple," in reference to the Vice President and his wife.[6] In a recent *Consumer Reports* test, several filtering programs also blocked sites on drug education, including the US National Institute on Drug Abuse.[7]

This leads to another topic for the educator: Which aspects of security are double-edged, and in which situations? Looking to history, we find examples of proactive security turned against its originators during World War II, when security services on both sides worked to turn captured spies into double agents (the British organization that did this was known as the Twenty Committee, for "XX" or "double cross").[8]

Legal issues

Teachers and their students can examine three key questions to reflect on the current state of US and international law, as well as the responsibilities of those developing security mechanisms.

The first arises from Sony's end-user license agreement (available at www.sysinternals.com/blog/sony-eula.htm), which raises several unusual issues. For example, it restricts consumers' use of any copies of the music on the CD, including requiring the installation of all updates (Article 8); forbidding them from taking the copy out of "the country where you reside" (Article 3, 1(e)); and having them to delete any copies if they file for bankruptcy (Article 9, 2-3) or if the CD is stolen (Article 9, 1 and 3). Are these reasonable restrictions? Moreover, can a vendor enforce unreasonable provisions if someone fails to read the EULA before accepting it? These are contract law questions, but they also raise questions of psychological acceptability, and they're critical to security.

Sony's actions are already facing at least two lawsuits, but our second question is whether a company that inserts a rootkit onto a user's system is likely to lose in court for doing so. Most students will see that the damage, or potential damage, caused by XCP raises the issue of leaving unsuspecting consumers open to external attacks. Further, you can argue that merely installing the mechanism modifies the kernel in undesirable ways and is, therefore, an attack.

To highlight the complexity of resolving these issues in our modern legal system, we suggest classroom exercises based on moot court scenarios, and involving law school students as well as typical computer science undergraduates, and individuals from other disciplines. In addition, students should consider the ramifications to them if, when writing kernel-modifying security mechanisms, they must be prepared to possibly defend them in court some day.

A third question, unasked (at least publicly) as of this writing, is whether the people who analyzed the XCP mechanism and the companies that developed ways to uninstall it are open to lawsuits. The issue here is the US Digital Millennium Copyright Act (DMCA), which bans the circumvention of access controls used to protect digital media and prohibits trafficking in tools designed to counteract mechanisms that enforce digital rights. The DMCA seems to place the researchers who analyzed XCP at legal risk, although they might be able to prevail in court and would face only civil penalties if they lost. The situation for companies such as Microsoft and Symantec, who are developing uninstall mechanisms and other countermeasures, would normally be much worse. The penalties for distributing such tools for circumventing digital rights' mechanisms range from civil fines of up to US$2,500 per tool distributed to criminal penalties. In this case, however, Sony is working with these antispyware companies, so they're unlikely to run any risk.

The Sony anticopying mechanism episode is a fiasco for several reasons. XCP modified many systems in ways that the owners didn't know and wouldn't likely have agreed to; it was intentionally difficult to remove; and it provided a hiding place for attackers. The publicity Sony received has far offset any benefits it accrued from the protection that the software provided.

Yet, from failure comes learning. Education builds on successes, but successes come after people learn lessons from myriad failures. The culture of hiding failure, of not bringing failure into the light, must change if we are to advance beyond it. Failures can lead to successes if educators can make the most of them. □

References

1. S. Cass, "Antipiracy Software Opens Door to Electronic Intruders," *IEEE Spectrum*, vol. 43, no. 1, 2006, pp. 12–13.
2. "Trojan Horse Exploits Sony DRM Copy Protection Vulnerability," Sophos, press release, 10 Nov. 2005; www.sophos.com/pressoffice/news/articles/2005/11/stinxe.html.
3. A. Kantor, "Sony: The Rootkit of All Evil?" *USA Today*, 17 Nov. 2005; www.usatoday.com/tech/columnist/andrewkantor/2005-11-17-sony-rootkit_x.htm.
4. M. Bishop, "Best Practices and Worst Assumptions," *Proc. 9th Colloq. on Information Systems Security Education*, 2005, pp. 18–25.
5. S. Caligirone and D. Frincke, "The Response Continuum," *Proc. 6th IEEE Information Assurance Workshop*, IEEE CS Press, 2005.
6. D. Einstein, "SurfWatch Strikes Gold as Internet Guardian," *San Francisco Chronicle*, 7 Mar. 1996, p. D–1; available at www.sfgate.com/cgi-bin/article.cgi?f=/c/a/1996/03/07/BU26606.DTL&hw=SurfWatch+strikes+gold+as+Internet+guardian&sn=001&sc=1000.
7. "Filtering Software: Better, but Still Fallible," *Consumer Reports*, June 2005; available at www.consumerreports.org/cro/electronics-computers/internet-filtering-software-605/overview.htm?resultPageIndex=1&resultIndex=1&searchTerm=web%20filters.
8. J. C. Masterman, *The Double-Cross System*, Avon Books, 1972.

Matt Bishop *is a professor in the department of Computer Science at the University of California, Davis, and a codirector of the Computer Security Laboratory there. His research interests include vulnerabilities analysis, the design of secure systems and software, network security, formal models of access control, and intrusion detection. He is the author of* Computer Security: Art and Science *(Addison-Wesley, 2002). Contact him at bishop@cs.ucdavis.edu.*

Deborah A. Frincke *is chief scientist for the Pacific Northwest National Laboratory's cybersecurity defense and response groups in Richland, Washington. She was previously a full professor at the University of Idaho, director of the Center for Secure and Dependable Systems, and cofounder of TriGeo Network Security. Her research interests emphasize system defense, especially intrusion detection, and the security of high-speed systems. Frincke has a PhD in computer science with an emphasis on computer security from University of California, Davis. Contact her at deborah.frincke@pnl.gov.*

The culture of hiding failure, of not bringing failure into the light, must change if we are to advance beyond it.