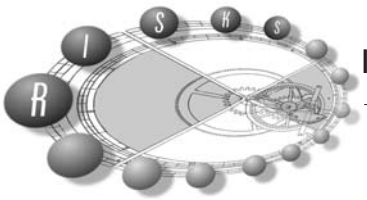

Secure Systems Conundrum

By definition, a secure system enforces some policy it is given. For example, such a policy might prevent confidential files from being revealed or might notify the copyright holder every time an MP3 file is played. The former protects the user as an individual; the latter enables new means of charging for electronically distributed intellectual property. Both might be seen as improving the status quo. Yet whether secure systems are in practice attractive really depends on two questions: What range of policies can the system enforce? And, Who chooses what policies the system enforces?

Automated policy enforcement mechanisms are incapable of showing good taste, resolving ambiguity, or taking into account the broader context in which a computer system exists. So formulating as a policy something that accurately reproduces our intents is likely to be impossible, and we must endure policies that conservatively block actions they shouldn't. One example involves system policies that disallow copying CDs containing music or software even though such copying is permitted by "fair use" provisions of copyright law. In general, intent is difficult to formulate precisely as a policy that can be enforced with a secure system—witness what happens in writing laws, which too often forbid or allow things society didn't intend.

The question of who chooses what policies are enforced? is tantamount to deciding who controls the system. On special-purpose devices (mobile phones and cable modems), enforcing policies imposed by others has not seemed offensive. Software on these devices is regularly updated and usage monitored without user consent (or knowledge). But enforce a policy to restrict what happens on a desktop system, and this system may no longer be general purpose. No surprise, then, that the Trusted Computing Platform Alliance (TCPA) and other efforts concerned with hardware and operating system support for secure computing systems are controversial. The surprise is that technical details are only a small part of the picture.

Today's computer users are either unwilling or unable to formulate nontrivial security policies for their desktop computers. So policies enforced by secure systems will likely come from third parties. We can only hope these will be consistent with our individual and collective best interests. What forces might bring this about? The law and the market seem the likely candidates.

The law arguably is not up to the task. Courts are having difficulty applying current laws to cyberspace—witness the debate associated with interpreting copyright's "fair use." Moreover, digital rights management is but one class of policies our secure systems might be enforcing. New laws might be the answer, but then recent U.S. (and some EU) experiences do not bode well for the public good.

Perhaps the market could provide the incentives. This, however, presumes a user or owner is free to choose which policy is enforced on a computer. It also presumes the market is open to would-be policy providers. Neither is guaranteed, and there are good reasons why neither might hold. The producer of a secure system has an incentive to provide a policy that prevents other policies from being added and other producers' software from being used.

Even if the computer owner were completely free to choose among policies, digital content providers will likely require certain policies to be present on any computer accessing their content. The free choice then becomes one of choosing between desired content and desirable policy—not much of a choice.

Insecure systems today allow users to circumvent copyright restrictions and license agreements. Sometimes this circumvention is done in ignorance; sometimes it's done in protest; but all too often it's done because the policy being enforced is clumsy and forbids something it shouldn't. In short, circumventing policy enforcement serves as a relief valve for clumsy policies.

Without a doubt, deploying secure systems has risks. Individuals are likely to suffer unless careful attention has been paid to who controls the policies these systems enforce and what values those policies reflect. And, if the so-called secure systems have vulnerabilities—as software so often does—malevolent users will still be able to do things they shouldn't, whereas ordinary users will have lost the means to compensate for clumsy policies. C

PAUL WATSON

Fred B. Schneider (fbs@cs.Cornell.edu) is a professor and director of the Information Assurance Institute at Cornell University.