It Depends on What You Pay

Fred B. Schneider

Today's computing systems are not very secure. Although we know how to build more secure systems, few seem willing to incur the additional costs. For users, these costs include fewer features, inconvenience (which would accompany more stringent authorization policies), and increased purchase price; for software producers, adding security means higher development costs and delayed time-to-market.

Instead of paying for system security, we end up paying for its absence. Breaches of confidentiality, data corruption, and service outages all have costs that are borne by businesses, their customers, and society at large. Perhaps better education of users and developers is the answer. Or maybe today's systems constitute a risk management "sweet spot," and damage from cyberattacks doesn't warrant the expense of better defense. However, our growing dependence on software and networked systems for critical infrastructures means that the expected costs of successful cyberattacks will soon soar—ignorance will become an expensive luxury; and the risk management sweet spot will vanish with the arrival of those low-probability, but high-cost, compromises.

Prudence then dictates that we create incentives to foster the development and adoption of more secure systems. We should strive for an economically efficient scheme: Profits should be apportioned according to risks, costs should be divided among the parties in a manner consistent with any benefits they enjoy, and most of what is paid should be used to increase security (rather than, say, to support the incentive scheme's enforcement).

Software producers are in business to make money. Increased profits are thus the obvious way to incentivize adding security. We might alter the demand side of the market, so that producers are able to sell secure systems at a higher price. Or we might alter the supply side, penalizing producers who market systems that aren't secure enough. Two mechanisms are available: government regulation and liability litigation. New legislation would be required for either, and avoiding legal costs and payments (either fines or damages) would become the incentive for both building secure software and deploying it.

What might those laws to incentivize secure systems proscribe? Our inability to measure the security of a system in a rigorous and principled way rules out the direct approach. Moreover, after decades of trying, there is reason to believe that developing a methodology to make such measurements is an extremely hard research problem. It remains a worthy goal, but we best not wait for the solution.

Stipulating that certain best practices be employed in system construction is a somewhat less attractive proxy, although regulating process rather than artifact has been successful in creating safe aircraft, for example. To go this route for secure software would require a generally accepted notion of what are "best practices" for creating secure systems. These best practices must be principled and not simply a recitation of what is being employed by one or another dominant producer.

Building from best practices was advocated as far back as 1991 in the US National Research Council's Computer Science and Telecommunications Board report *Computers at Risk: Safe Computing in the Information Age*, and as recently as the most current version of the Common Criteria. None of these attempts has gained traction, however, and the reasons for this are not clear.

One thing is clear, though: Better security has a cost, and somebody will have to pay—the government (and ultimately taxpayers), the consumer (paying higher prices), or corporate investors (through lower return on investments). Moreover, no party will be enthusiastic about making investments to improve system security without some means to understand the value those investments add. Education will help and pay off in other ways too, but developing an objective and principled basis for measuring system security would be my choice as the means to enable an economically efficient market that incentivizes trustworthiness.

So why be stingy?
It depends on what you pay!
—*The Fantasticks* by Tom
Jones and Harvey Schmidt □