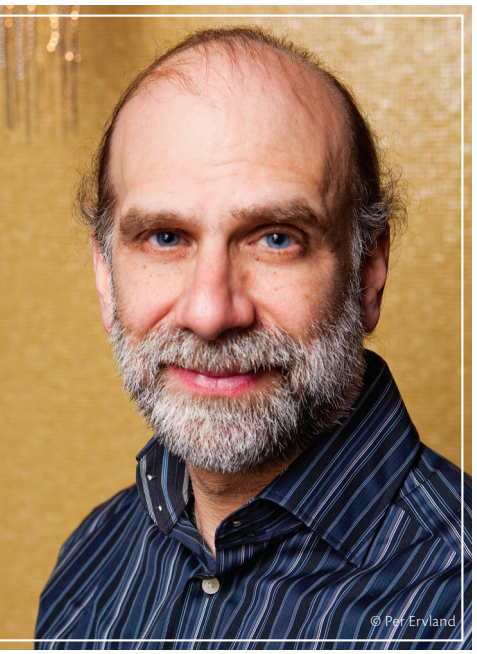

Bruce Schneier
BT

How Changing Technology Affects Security

Security is a tradeoff, a balancing act between attacker and defender. Unfortunately, that balance is never static. Changes in technology affect both sides. Society uses new technologies to decrease what I call the *scope of defection*—what attackers can get away with—and attackers use new technologies to increase it. What's interesting is the difference between how the two groups incorporate new technologies.

Changes in security systems can be slow. Society has to implement any new security technology as a group, which implies agreement and coordination and—in some instances—a lengthy bureaucratic procurement process. Meanwhile, an attacker can just use the new technology. For example, at the end of the horse-and-buggy era, it was easier for a bank robber to use his new motorcar as a getaway vehicle than it was for a town's police department to decide it needed a police car, get the budget to buy one, choose which one to buy, buy it, and then develop training and policies for it. And if only one police department did this, the bank robber could just move to another town. Defectors are more agile and adaptable, making them much better at being early adopters of new technology.

We saw it in law enforcement's initial inability to deal with Internet crime. Criminals were simply more flexible. Traditional criminal organizations like the Mafia didn't immediately move onto the Internet; instead, new Internet-savvy criminals sprung up. They set up websites like CardersMarket and DarkMarket, and established new organized crime groups within a decade or so of the Internet's commercialization. Meanwhile, law enforcement simply didn't have the organizational fluidity to adapt as quickly. Cities couldn't fire their old-school detectives and replace them with people who understood the Internet. The detectives' natural inertia and tendency to sweep problems under the rug slowed things even more. They spent the better part of a decade playing catch-up.

There's one more problem: defenders are in what military strategist Carl von Clausewitz calls "the position of the interior." They have to defend against every possible attack, while the defector only has to find one flaw that allows one way through the defenses. As systems get more complicated due to technology, more attacks become possible. This means defectors have a first-mover advantage; they get to try the new attack first. Consequently, society is constantly responding: shoe scanners in response to the shoe bomber, harder-to-counterfeit money in response to better counterfeiting technologies, better antivirus software to combat new computer viruses, and so on. The attacker's clear advantage increases the scope of defection even further.

Of course, there are exceptions. There are technologies that immediately benefit the defender and are of no use at all to the attacker—for example, fingerprint technology allowed police to identify suspects after they left the crime scene and didn't provide any corresponding benefit to criminals. The same thing happened with immobilizing technology for cars, alarm systems for houses, and computer authentication technologies. Some technologies benefit both but still give more advantage to the defenders. The radio allowed street policemen to communicate remotely, which increased our level of safety more than the corresponding downside of criminals communicating remotely endangers us.

Still, we tend to be reactive in security, and only implement new measures in response to an increased scope of defection. We're slow about doing it and even slower about getting it right. ■

Bruce Schneier is the chief security technology officer of BT. This essay was excerpted and adapted from his new book, *Liars & Outliers: Enabling the Trust that Society Needs to Survive* (www.schneier.com/lo). He can be found online at www.schneier.com.

Copublished by the IEEE Computer and Reliability Societies