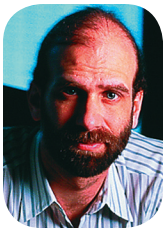
Security and Function Creep

Security is rarely static. Technology changes the capabilities of both security systems and attackers. But there's something else that changes security's cost/benefit trade-off: how the underlying systems being secured are used. Far too often we build security for one purpose, only to find it being used for another purpose—one it wasn't suited for in the first place. And then the security system has to play catch-up.



Bruce Schneier
BT

Take driver's licenses, for example. Originally designed to demonstrate a credential—the ability to drive a car—they looked like other credentials: medical licenses or elevator certificates of inspection. They were wallet-sized, of course, but they didn't have much security associated with them. Then, slowly, driver's licenses took on a second application: they became age-verification tokens in bars and liquor stores. Of course the security wasn't up to the task—teenagers can be extraordinarily resourceful if they set their minds to it—and over the decades driver's licenses got photographs, tamper-resistant features (once, it was easy to modify the birth year), and technologies that made counterfeiting harder. There was little value in counterfeiting a driver's license, but a lot of value in counterfeiting an age-verification token.

Today, US driver's licenses are taking on yet another function: security against terrorists. The Real ID Act—the government's attempt to make driver's licenses even more secure—has nothing to do with driving or even with buying alcohol, and everything to do with trying to make that piece of plastic an effective way to verify that someone is not on the terrorist watch list. Whether this is a good idea, or actually improves security, is another matter entirely.

You can see this kind of function creep everywhere. Internet security systems designed for informational Web sites are suddenly expected to provide security for banking Web sites. Security systems that are good enough to protect cheap commodities from being stolen are suddenly ineffective once the price of those commodities rises high enough. Application security systems, designed for locally owned networks, are expected to work even when the application is moved to a cloud computing environment. And cloud computing security, designed for the needs of corporations, is expected to be suitable for government applications as well—maybe even military applications.

Sometimes it's obvious that security systems designed for one environment won't work in another. We don't arm our soldiers the same way we arm our policemen, and we can't take commercial vehicles and easily turn them into ones outfitted for the military. We understand that we might need to upgrade our home security system if we suddenly come into possession of a bag of diamonds. Yet many think the same security that protects our home computers will also protect voting machines, and the same operating systems that run our businesses are suitable for military uses.

But these are all conscious decisions, and we security professionals often know better. The real problems arise when the changes happen in the background, without any conscious thought. We build a network security system that's perfectly adequate for the threat and—like a driver's license becoming an age-verification token—the network accrues more and more functions. But because it has already been pronounced "secure," we can't get any budget to re-evaluate and improve the security until after the bad guys have figured out the vulnerabilities and exploited them.

I don't like having to play catch-up in security, but we seem doomed to keep doing so. □

Bruce Schneier *is chief security technology officer at BT. Read his blog at www.schneier.com.*

cn *Selected CS articles and columns are also available for free at http://ComputingNow.computer.org.*