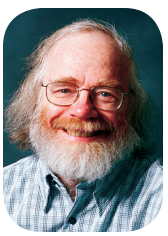
Security as a Systems Property

Periodically, someone *knows* what to do about cybersecurity. It might be encryption, firewalls, patches, formal methods, more open source, less open source, better law enforcement—you name it. Everyone is right, in that their solutions will sometimes help. More accurately, though, everyone is wrong: their ideas might be *part* of the solution, but there is no single answer. Security is a *systems* property; attacking the problem piecemeal will lead only to frustration.



STEVEN M. BELLOVIN
Columbia University

What do I mean by a "systems property"? Just that—what matters is not whether any individual piece is strong or weak but rather whether the bad guys can get in somewhere. By definition, a system is composed of many different components; any of them could be weak. As I tell my students, "You don't go through strong security, you go around it."

People ignore this all too often. They'll spend millions of zorkmids on the latest and greatest VPN but ignore the fact that the laptops their employees use to connect are frequently used by their employees' teenagers to visit dubious places on the Net. They'll install a firewall with 17-factor authentication but then forget they've made access to email so inconvenient that employees will simply forward their corporate address to some ad-driven freemail system.

Nowhere is this tendency more evident than in voting schemes. Over the years, handwritten paper ballots have been replaced successively by official, preprinted ballots, lever and punch-card machines, direct-recording electronic (DRE) systems, DRE systems with paper trails, and—now—optically scanned, computer-prepared, paper ballots. Successive schemes have always been touted as "more secure" (as well as faster and cheaper), but are they? Each system has had its failings. Ballot boxes can be stuffed. Lever machines jam (sometimes intentionally) and are easily readable in mid-election by anyone who removes the cover. Arguably, the weaknesses of punch-card systems determined the outcome of the 2000 US presidential election. DRE systems are heir to all of the weaknesses of software. And optically scanned paper ballots? They illustrate my point.

The putative advantage of any paper-based voting system is that there's something to recount, by hand if necessary. But when are recounts "necessary"? The standard answer, often enshrined in law, is that recounts are done only in close races. That's insufficient—recounts of a random subset of precincts have to be done routinely, as a check on the correctness of the automated system. Without that, they provide little security advantage. In other words, routine, random recounts are part of the system, and must be treated as such.

How, then, do we protect systems? The answer is straightforward: each component must be evaluated independently and protected as necessary. Beware the easy answers, such as deploying stronger encryption while ignoring, say, vulnerable end points; that's too much like looking under the streetlamp for lost keys, not because they're likely to be there but because it's an easy place to search. Remember, too, that people and processes are system components as well, and often the weakest ones—think about phishing, but also about legitimate emails that are structurally indistinguishable from phishing attacks. I'm not saying you should ignore one weakness because you can't afford to address another serious one—but in general, your defenses should be balanced. After that, of course, you have to evaluate the security of the entire system. Components interact, not always in benign ways, and there might be gaps you haven't filled.

Systems are far more powerful and flexible than isolated computers, but they're also more vulnerable; our security practices must recognize this. □

Steven M. Bellovin *is a professor of computer science at Columbia University. Contact him via www.cs.columbia.edu/~smb.*

Authorized licensed use limited to: Columbia University. Downloaded on December 15, 2009 at 13:38 from IEEE Xplore. Restrictions apply.