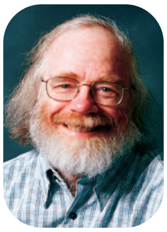
Security and Privacy: Enemies or Allies?

It is, we are told, a dangerous world. Hackers have infiltrated our computers. Identity thieves make our financial lives miserable. Worst of all, terrorists are daily plotting evil deeds. What is to be done?



Steve Bellovin
Columbia University

Part of the solution, it seems, is a massive invasion of privacy. We are asked for all manner of personal data before engaging in transactions that were once routine. We show ID cards at every juncture. Is this necessary? Is it helpful? Or is it actually harmful, not just to our privacy but to security as well?

I'm not talking about the trivially nonsensical manifestations of this syndrome. We've all been asked to show a picture ID by someone who does nothing with it but verify that we have such a document. No reference is made to any external data that might, say, identify the bearer as a known bad guy. For that matter, the inspector rarely, if ever, even tries to compare the picture to the person. The assumption seems to be that your driver's license somehow has a field that indicates "Evildoer: true" or "Evildoer: false." Usually, this sort of activity is harmless, but it conditions people to believe it provides real security, thus displacing any actual protective measures.

The problem I'm concerned about is deeper. Doing any sort of identity-based security screening requires access to back-end databases, but the existence of these databases isn't just a potential privacy issue, it's a security problem as well.

The problem is simple: data that exists can be stolen and misused. If the data is security-sensitive, its misuse has security implications. Assume, for example, that a would-be terrorist obtains a copy of an airline's watch list. It takes no imagination to see the next step: find a recruit whose name isn't listed.

Other databases pose other threats. Obviously, any bank account record provides all the information needed for identity theft, but it also provides a good conduit for various forms of money-laundering. Credit-card spending records can, in many cases, be used for extortion: think of the things some people buy that they wouldn't like to be public knowledge.

Everybody knows by now that such databases can't be kept secure. Nor is there any single cause for such breaches; databases have been lost via fraud, employee malfeasance, and simple carelessness with backup tapes.

It's hard to avoid the conclusion that the very existence of such databases creates concrete problems, but is there an alternative?

One answer, of course, is encryption. Encryption does little to prevent insider abuse; if used properly, however, it's a powerful weapon against bulk compromise of data. Beyond that, there is a powerful arsenal of techniques that can be used to create privacy-preserving databases. Indeed, a large body of research is dedicated to privacy-preserving data mining. Yet few of these schemes have been used in the real world. Perhaps it's time to give them a try. The intelligence community has long since learned the value of code names and the like to help protect the identities of agents. They've also learned—the hard way—what an Aldrich Ames or a Robert Hansen can do with accumulated data.

Some records are, of course, irreplaceable; they must exist, and no anonymity techniques can protect them against misuse. But we can do without some of the others. Sometimes, we need clever cryptography; more often, we need to step back and ask if the database really needs to exist. Otherwise, we will just have to live with the threats they pose, not to privacy but to security. □

Steve Bellovin is a professor of computer science at Columbia University. His research interests are networks, security, and especially why the two don't get along. He received a BA from Columbia University and an MS and PhD in computer science from the University of North Carolina at Chapel Hill. He helped create netnews, or usenet news, and for this achievement, he was awarded the Usenix Lifetime Achievement Award. Bellovin is coauthor of Firewalls and Internet Security: Repelling the Wily Hacker. *Contact him via www.cs.columbia.edu/~smb.*