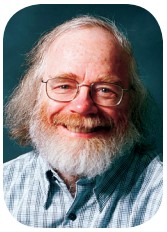
Identity and Security

People raise the issue every few years: "If only," they say, "the Internet had strong identification, we wouldn't have so many security problems. Perhaps we can reinvent the Internet to correct that mistake." It won't work. First, even if we did, we can't have strong, useful identification. Second, having such identification would cause bad side-effects. Third, and most important, it couldn't solve the problems. Although we don't know what a solution might look like, we know where it has to fit—and it isn't in the box labeled "identity."



Steven M. Bellovin
Columbia University

A strong identification system presupposes a strong notion of identity. The Internet, though, is multilayered; identity is different at each layer. My computer has three different MAC addresses and several IP addresses, including many IP addresses and logins for different instant message systems. If I switch computers, locations, or employers, several of these would change. Am I no longer myself? Sophistry, some would say; those could all be temporarily bound to my "real" identity. In that case, we already have pretty strong identification, in the combination of time stamp, IP address, and log files.

Suppose, though, that we really do want strong identification; we're even going to digitally sign every packet. Someone, of course, has to issue the credentials. Who should it be? Would the US government trust credentials issued by China? Would the Chinese government trust American credentials? The answers to the last two questions, of course, are a resounding "no."

Even if we could move past the credentialing problem, how do we handle what I call "proxy packets"? If I send you mail, it goes from my laptop to an organizational mail handler that serves thousands of users. It sends my mail to your organization's inbound mail handler; in turn, your computer picks up the email. But that middle hop, from mail handler to mail handler, can't be signed by my key; how can the mail—perhaps virus-infected—be attributed to me at that level? The answer is the logs on the sending system, but if we have those logs, we don't need signed packets.

Assume, however, that we can make all that work. We have now created serious privacy problems. I'm certainly willing to let the government trace my packets in pursuit of an actual, identified criminal. I might be willing to have it make records preemptively, in the hope of deterring or catching future attackers. But I'm certainly not willing to let the megacorporations of the world track my every step through cyberspace. Web cookies and local stored objects are bad enough; I don't need another form of identification that I *can't* turn off. Maybe we can use clever cryptographic techniques to prevent that; however, the whole scheme is useless if there's no way to uncover the real person behind the packets. What policy should control that? If the government of Freedonia wants to unmask my identity, is it to trace a real cyberattack, harass or block me for my political beliefs, or simply to sell the information to a Freedonian multinational? And if we can't solve that, how can we expect to trace back attacks coming from Freedonia?

Perhaps there's a good answer to that one, too. Maybe some miraculous cryptographic solution does exist, with anonymous credentials and proxy signatures and honest international cooperation—but it still won't work. Most online misbehavior comes from hacked machines; in turns, these machines have been hacked because of buggy code. Strong authentication is useful in many circumstances, but the bad guys don't have to go through the authentication system—they simply go around it. A strongly encrypted, strongly authenticated connection between a hacked machine and another target still lets the bad guys in, whereas identification does nothing but mislead the good guys. In other words, identification will be useful only when we don't need it because we've solved the computer security problem. □

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