How to Improve Security?

It takes more than flossing once a year.

Dear KV,

We recently had a security compromise at work, and now the whole IT department is scrambling to improve security. One problem this whole episode has brought to light is that so much security advice is generic. It's like being told to lock your door when you go out at night, without saying what kind of lock you ought to own or how many are enough to protect your house. I think by now most people know they need to lock their doors, so why aren't there more specific guidelines for securing systems?

Scrambling

Dear Scrambling,

While you complain about how the advice you're getting is generic, your letter also lacks any level of detail. You don't say what kind of security problem you had or what steps are being taken to deal with it.

I think one of the reasons so much security advice comes across as generic is that the people who write it have come to the realization that, like a dentist, their advice is usually ignored, or, if not ignored, heeded for only a short period of time.

Every year I go to the dentist, and every year he tells me I should brush and floss. I have been brushing my teeth since I was a little kid, but I never flossed. Each year, after my dentist again gives me the very sound advice to floss my teeth, I do—for about a week, or maybe two. Inevitably I forget once, then twice, and then I fall out of my one- or two-week habit and don't floss again until after my next visit to the dentist.

Much of the advice around properly securing systems is about changing how we use our computers, and, from the point of view of most users, it only introduces more work without an obvious, visible benefit. If I make a system run faster, that's obvious to the user, but if I make a system more secure, that's visible only if there had been a security problem. This is one of the key reasons that security concerns are usually left out of most systems unless that system has a history of being attacked. Banks are a good example. While it is quite obvious that many banks have not sufficiently thought out the threats to their systems, it is also the case that if you ask someone who works in a bank what a big risk to their system would be, they're pretty likely to list theft in the top three. Of course theft is obvious, but, in part, it's obvious because it has been the case for most of human history.

The idea of theft of information, or the idea that information might be valuable, became important to the average person only with the modern invention of credit. Before the 20th century most people thought about the theft of information—if they thought about it at all—as it related to military secrets, such as plans for weapons, the strength and placement of armies, and the plans for attack and defense of military positions. Unless you were wealthy or famous, your name, for example, was not valuable in and of itself. The advent of credit-based payment schemes and their extension to the Internet changed all of this.

FIGURE 1

Dictionary Attack on a Server

```
Jul 10 03:32:15 xxxxxxx sshd[95851]: Invalid user aadriano from 189.1.64.48
Jul 10 03:32:16 xxxxxxx sshd[95853]: Invalid user aaghie from 189.1.64.48
Jul 10 03:32:18 xxxxxxx sshd[95855]: Invalid user aaron from 189.1.64.48
Jul 10 03:32:21 xxxxxxx sshd[95857]: Invalid user aaron from 189.1.64.48
Jul 10 03:32:23 xxxxxxx sshd[95859]: Invalid user aaron from 189.1.64.48
Jul 10 03:32:24 xxxxxxx sshd[95861]: Invalid user abba from 189.1.64.48
Jul 10 03:32:26 xxxxxxx sshd[95863]: Invalid user abba from 189.1.64.48
Jul 10 03:32:28 xxxxxxx sshd[95865]: Invalid user abba from 189.1.64.48
```

There is another fact that makes it easy not to think about securing computer systems—the attacks on them go unseen by most people. How many people, even in the technology industry, ever see the logs from their Internet-connected servers that show the near-constant attempts of attackers to gain access?

Figure 1 shows a common dictionary attack on a server—one that can be partially mitigated by greylisting the IP addresses from which these connections originate. Such attacks occur constantly, day and night, and are usually launched from systems that have themselves been breached elsewhere on the Internet.

Attacks on banks—to continue my previous example—once required the robber to show up in person: either during the day, guns blazing; or at night, tunneling into the vault. Attacks on computers over the network can be, and are, launched from anywhere there is a network connection, anywhere in the world, and they don't start out with someone yelling, "This is a holdup! Shut up, get on the floor, and nobody gets hurt."

I actually find the term *security compromise* amusing. A compromise is defined as "an agreement or a settlement of a dispute that is reached by each side making concessions." But when a security compromise is not reached by each side making concessions, it is most often reached because one side, the victim, has failed to take adequate precautions.

So what should you do after a security breach? I could tell you the same things that you'll find on reputable security sites, such as the SANS Institute (<http://www.sans.org/>), but I won't do that here. After all, do you floss after you brush your teeth? I do, for one week a year.

KV

KODE VICIOUS, known to mere mortals as George V. Neville-Neil, works on networking and operating system code for fun and profit. He also teaches courses on various subjects related to programming. His areas of interest are code spelunking, operating systems, and rewriting your bad code (OK, maybe not that last one). He earned his bachelor's degree in computer science at Northeastern University in Boston, Massachusetts, and is a member of ACM, the Usenix Association, and IEEE. He is an avid bicyclist and traveler who currently lives in New York City.

© 2011 ACM 1542-7730/11/0800 \$10.00