by Gary McGraw

Is Security Really About Getting Nothing Done?

The biggest problem in computer security is that people just want to get their jobs done. If people were content to do nothing, then we wouldn't have any security problems. Dumb, but effective.

The right kind of security allows people to do their work without giving away the farm. The only way to do this is to really understand what it is that people need to get done and then limit them to doing only that. This all sounds a bit draconian—after all, you're probably not supposed to be buying books or listening to MP3s at work, are you? But believe me, security doesn't exist to make your life dull.

The crux of the problem is that we started with the universe of all possible things, and we've slowly been attempting to remove the dangerous things from that pile one at a time ever since. (Sounds like a job for Sisyphus, if you ask me.) At the root of this is the concept of default permit.

Default permit is the idea of starting with everything "on" and only turning off what's dangerous. That doesn't work. Too much danger lurks out there. In fact, the list of all possible dangerous things is infinite. In order to follow the principle of least privilege, you need to start with no privilege at all and add things only as necessary. This is called default deny. The trick to making default deny work in practice is to have a solid handle on what people actually need to do to get their work done, then let them do that and nothing else.

The trusty sidekick of default permit is the black list. Marcus Ranum, firewall inventor and security curmudgeon, gives both concepts the top two slots in his "The Six Dumbest Ideas in Computer Security" (see www.ranum.com/security/computer_security). Creating a list of known bad things isn't a good foundation for security. Anti-virus systems today have insanely large lists containing over 75,000 viruses, worms, and other malware. These lists grow daily and require constant care and feeding, yet they don't even begin to stop creative new attacks. The problem is that blacklisting doesn't work. Why? Ever try writing down an infinitely long list? It takes forever. Instead, think about specifying (in a white list) what should happen, then make sure only those things ever happen.

The concept of default deny must be applied much more widely than to anti-malware and firewall rules. (For an explanation of why those are good ideas, see last month's column "How Bad Is Intrusion Detection?" and September 2004's Soapbox "No Default Deny? Disaster!" at www.ITarchitect.com. Search for Doc ID# 2010security and 1909soapbox, respectively.) When push comes to shove, how many programs do you really need to run on your PC? Try making a list. It may surprise you how short it is, even if you do count the MP3 player. By applying default deny to your PCs, you could make a large part of your security risks more manageable.

This isn't just a theoretical pipe dream. Years ago Cigital Labs created a whitelisting solution called the Execution Management Utility for a certain government customer, and Microsoft has even built some execution limitation ideas into Windows XP. There are some remaining issues, but by and large we would all be better off running a fixed set of programs.

> “By applying default deny to your PCs, you could make a large part of your security risks more manageable.”

That's software, but what about people? Default deny is applied to people all the time. Bank tellers are allowed to carry out only a small set of possible transactions. Receptionists' duties are defined in terms of tasks such as answering the phone, sorting the mail, and so on, but we almost never write down a list of what they're not supposed to do (sign merger papers, for example). Of course, there'll always be situations that are ambiguous or tricky, but that's what makes security challenging and fun.

Gary McGraw is CTO of Cigital, a software quality management consultancy. He is co-author of *Exploiting Software* (Addison-Wesley, 2004), *Building Secure Software* (Addison-Wesley, 2001), and *Java Security* (Wiley, 1996). Reach him at gem@cigital.com.