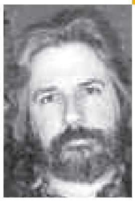
ROBERT G. FERRELL

/dev/random



Robert is a semiretired hacker with literary and musical pretensions who lives on a small ranch in the Texas Hill Country with his wife, five high-maintenance cats, and a studio full of drums and guitars.

rgferrell@greatambience.com

WE ALL GET BEES IN OUR BONNETS from time to time, and one little critter that's been buzzing around in mine for quite a spell now is the gradual disappearance of the concept of personal responsibility. Growing up in West Texas, when you made a mistake you stared down at the ground and scraped your toe in the sand in embarrassment for a few seconds, wishing that teleportation weren't just a cheesy sci-fi effect, then straightened your back, squared your shoulders, and took the consequences. Sure, we occasionally produced stink beetles who tried to blame missing that easy pop fly to center field on the sun being in their eyes or getting distracted by one of those balsawood glider–sized dragonflies endemic to the area, but by and large folks in my neck of the cactus plantation had a pretty firm grasp on societal cause and effect. OK, I think I've got all the bugs out of my system now. Did I mention how much I hate big red wasps?

The fundamental idea that *you*, not some corporation/neighbor/government agency/supernatural influence/alignment of fantastically distant celestial objects, are responsible for what happens to you has apparently joined the Ivory-billed Woodpecker and the woefully misnamed "common sense" on the critically endangered list. I suppose such quaint and outdated mores simply don't resonate with today's society, working as they do in opposition to the generation of new SUVs and beach properties for the legal profession.

Some examples of total abdication of personal responsibility are obvious, such as the recent spate of well-publicized lawsuits over fumble-fingers who scald themselves with beverages, consumers who take that term a bit too literally and wolf down anything and everything put in front of them, blaming the food vendors when this indiscriminate consumption results in arteries with the structural characteristics of uncooked pasta, and parents who think the rest of the world should be held accountable for their own inability to control what their children read and watch on a daily basis. Others are more insidious: every computer sitting at the terminus of an always-on broadband Internet link, for example.

Imagine that you buy a new car and leave it, unlocked and running, in your driveway 24 hours a day. Imagine further that some lowlife slithers up, steals said car from said driveway, and employs it in the commission of a crime. Do you share any of the blame for this event? You didn't actively participate in or condone the action itself, so why would you? Is providing easy access to a potent tool acting as a sort of unwitting accessory to the crime? The legal arguments surrounding this scenario are more complex than they may first appear, and let me state now for the record that I Am Not A Lawyer (I prefer to sleep at night), but fundamentally this boils down to a question of personal responsibility, however oblique that may seem to the case as stated.

Items deemed by expert consensus to be potentially dangerous to health or safety are ideally accessible only by those who bear the brunt of responsibility for their use. This includes weapons, prescription drugs, vehicles, theatrical adaptations of classic comic books, and . . . computers. That's right: computers. A potential for economic and sociological mayhem, if not actual public safety concerns, resides right there in that oversized shoebox sitting on edge under your desk. Whether or not you admit it, if you don't take some fairly simple steps to keep out the riffraff it is almost a dead certainty that your computer will be recruited into a multicellular evil entity whose metabolic functions are anything but beneficial to the society on which they ravenously feed. I liken botnets, as these infernal networks are called, to digital cancers. They spread one cell at a time throughout a logical system until most or all of the CPU cycles of that system are devoted not to their original benign purpose (I'm being charitable here, I realize) but to the propagation of the infection and the bidding of their demonic overlord(s). Or mayhap your box will be hijacked to serve as an anonymizing launch pad for malicious activity such as identity theft or reading celebrities' text messages to their dog groomers. Either way, that PC you rely upon for delivering your spam and checking your online sports memorabilia auctions will become just one more hapless cog in a larger, sinister enterprise—I mean, in addition to already being part of the Internet.

So, you may well ask, what does that have to do with personal responsibility? The answer, my friend, is simple in the end: everything. Ultimately, you are responsible for what gets done using your hardware. It's *your* computer, in *your* house, on a network *you* pay to access. If you don't understand how to keep it secure because you're *nontechnical*, fine: Outsource that job to someone you trust. Simply throwing up your hands and claiming exemption because you don't understand the issues or technology involved does not wash. Do you understand the myriad mechanical, chemical, and physical processes that take place when you drive your car? Probably not. Does that make you any less liable when you plow through a crowd drinking coffee at a sidewalk café? No. It is implied by your assumption of the role of pilot of a motor vehicle that you have received basic instruction in the safe operation thereof.

So it should be with the increasing potential hazard that is the Internet. Millions of people all around the globe depend on you to do your small part to minimize the spread of malware. It doesn't take much—a few mouse clicks in most instances and a basic policy of not opening attachments unless you're absolutely certain of their origin and contents—to prevent 99% of all commonly encountered exploits. As with automobiles, the benefits of learning to operate the machine safely exceed the effort required by several orders of magnitude. The ROI, in other words, be phat. The penalties for irresponsible computing so far have been diffuse and applied too far up the chain to do much good. The effort has to come from end users like us to be successful. Put another way:

> Take it to the house y'all, lock it or lose it.
> Don't leave it in the open 'cause the thugs'll abuse it.
> Close it off, shut 'em down, make 'em find another kill'n.
> The botz take you down unless you get physical.

Here, then, is my Contract with the Digerati: If I don't see a marked decrease in DDoS and other botnet-related activity in the near future, I'll pen more of these, uh, lyrics. I don't think you want that, now, do you? I knew you didn't. I could see it in your eyes.

But, you protest, I'm an inherently superior UNIX user and savvy enough to secure my own systems. Cleverly, I'm counting on that. It leaves you free to devote yourself to helping those less technically blessed to secure theirs. Now get to work, slackers. Don't make me come over there. Dword?

SIGNS OF INTRUSION-- PERHAPS A KERNEL EXPLOIT!
HMMM
WHAT DID THEY DO WHEN THEY FOUND THE INTRUSION?
DID THEY MONITOR THE NETWORK?
NO! THEY CAPTURED SOME DATA AND SHUT IT DOWN.
R. Moon

Copyright 2006 R. Moon