ROBERT G. FERRELL

/dev/random

Robert G. Ferrell is an information security geek biding his time until that genius grant finally comes through.

rgferrell@gmail.com

I SPENT, ALL TOLD, ABOUT NINE HOURS this weekend in the saddle of a zero-turn-radius beast (Ol' Yeller) doing some of the fall mowing of my property east of San Antonio. All that time dodging choking dust clouds, aggressive insects, and haphazardly flung vegetation gave me ample opportunity to contemplate the current state of information security—which is, as usual, dismal.

If this seems an unreasonably pessimistic appraisal, spend a few minutes perusing any periodical or Web site devoted to infosec and you must quickly come to the same conclusion. The reasons for this sad state of affairs are myriad: poor security engineering practices, failure on the part of corporations and government institutions to collect and analyze security-relevant operating system events, little or no network filtering/packet inspection, appalling Internet hygiene, and world-class gullibility being among the most prominent.

Besides the host of obvious issues, however, there is an insidious nest of more subtle creepy-crawlies squirming beneath the floorboards. One of these abominations recently raised its misshapen head and wriggled behind the wainscoting, there to bore yet more holes in the already sagging load-bearing timbers of our information economy. I refer—in case you're wondering where, if anywhere at all, I was going with this tortured metaphor—to security flaws masked as marketing strategies.

The latest half-baked idea from a popular microprocessor vendor, wherein they will sell you a processor that only functions as designed *after* you've purchased an additional code to unlock the crippled parts, is quite possibly the most offensive and ill-conceived travesty since the Digital Millennium Copyright Act in one fell swoop made *a priori* criminals of most of the entertainment-consuming population. Every time I think high-tech marketing can't possibly get any more inane it suddenly does, and without even breaking a sweat.

The problem with proprietary hardware and software is that you really don't know what you're purchasing. We as consumers long ago bought into the "we can't tell you how it works because that's a trade secret" corporate philosophy lock, stock, and barrel under the cover of free market capitalism; now we're stuck with the consequences of this appalling lack of collective judgment. The area where the black box principle takes one of its

heaviest tolls on society is security, or, rather, the profound absence thereof. Let's employ one of the most familiar and ironic of all Internet polemic tools to examine this: a reference book known as "The Dictionary," as though, *Highlander*-esque, there can be only one. Mine defines *security* this way: "The quality or state of being secure: as: (a) freedom from danger: safety; (b) freedom from fear or anxiety." It is the latter meaning I want to address here.

Fundamentally, anxiety is the absence of contentment. If you are satisfied with things the way they are, you aren't going to be anxious. Contentment itself can be brought about by following either of two protocols: (1) be certain that everything is going your way; (2) simply don't care whether it is or not.

Threading our way back up this chain of reasoning to the original stated premise, then, one path to security is apathy. That is the path the vast majority of computer users choose to take. Security means never having to say you bothered.

How does this relate to the vending of broken microprocessors? Hear me out. The manufacturer says the code they will gladly sell you to un-hobble the processor you've already paid for (apparently that initial outlay is merely a deposit) unlocks more level 2 cache and hyperthreading. Fine. That's just the part they're *telling* you about. What else is crippled, either intentionally or as a victim of collateral damage? You don't know? Neither do I. That uncertainty should trigger all sorts of alarms about potential security flaws but it won't, because *not caring is not worrying.* Security by apathy. Don't worry, be hapless.

Black boxes function or they don't, but this is not for you and me to question or influence. To paraphrase Arthur C. Clarke, any sufficiently obfuscated technology is indistinguishable from magic. Vendors are effectively telling us not to worry about how their products function: it's magic and you wouldn't understand, anyway. Trust us to have baked robust security right in. No, we won't reveal exactly what kind of security it is, but believe us, it's like really, really secure.

Let's take a little flight of fancy here (please limit your carry-on items to two per passenger) and imagine what might happen if this marketing philosophy were extended to other types of security-related consumer goods.

[*Wavy dissolve to smiling, attractive blonde holding brightly-colored product package*]

Congratulations on your purchase of a new EverJam 9000 Burglar-Proof Padlock. Enclosed in the packaging you will find a coupon for 10% off on the optional EverKey Pro Upgrade that allows you to open your new lock at any time, rather than once per day. Please do not read the warranty waiver, then sign, date, and return in the postage-paid envelope.

[*Quick wipe to photo montage of serene meadows full of flowers*]

Thank you for choosing the Cochlea Blaster Home Security System, now with extra-strength Decibels. Please call 1-888-URPUNKD to activate your account. Have your account identifier, birth certificate, three major credit cards, bank routing number, Social Security card, and blood type ready. At the prompt, press "1" for 24-Hour Monitoring (additional charge applies); press "2" if you want the optional "Manual Silencing" package (additional charge applies); press "3" if you want to disable "No Open" notifications (additional additional charge applies).

I could go on, but the equine is beginning to stiffen up.

[*Fade to black*]