/dev/random

ROBERT G. FERRELL

Robert G. Ferrell is a fourth-generation Texan, literary techno-geek, and finalist for the 2011 Robert Benchley Society Humor Writing Award. rgferrell@gmail.com

I am not a computer scientist. I don't designs 'em, I just runs 'em. When talk 'round the cocktail party buffet table turns to B-trees, linked lists, and why bubble sorts are awful, I grab another stuffed jalapeño and look for a less esoteric knot in which to mingle. Consequently, I am in no position to pontificate with authority or even basic coherence on any topic that contains a CS-related word more advanced than "algorithm." I had probably been a sysadmin for ten years before I learned what *that* one meant.

Computer science and systems administration are very different disciplines. Whenever I see a job opening for a system administrator that lists as one of its requirements an undergraduate degree in computer science, I roll my eyes and write that company, or at least their HR department, off as *personae sans clue*. Requiring a CS degree for your sysadmins is like insisting a Formula 1 driver possess a degree in traffic engineering. It's essentially a non sequitur. I think I've ranted on this before.

We used to joke that the only truly secure system was one with no I/O devices that had been encased in concrete and dumped into the Challenger Deep. Apparently that was no joke. Recent events have shown us that any system connected to another not only *can* but eventually *will be* compromised. I would now go so far as to say if you have *ever* used a credit card, applied for a US security clearance, or shopped online, your information is available to anyone who cares to purchase access to it. You and I and virtually everyone you know have been, to bring the subject into sharp focus, quite thoroughly pwned.

Prior to becoming a full-time writer I made my career, such as it was, in information security. Back in those days we naively believed that, were proper precautions taken and best practices followed faithfully, you could operate an enterprise-level network in relative safety where the vaunted C-I-A (confidentiality, integrity, and availability) were concerned. It's become increasingly obvious over the past few years, however, that networking is rotten at its most fundamental core, security-wise, and can't be fixed. I think the only sensible way to proceed from this point forward is to assume that every single bit of data you place in any networked environment will be, without any realistic possibility of sanctuary, compromised.

My personal solution, were money and profound inconvenience no obstacles, would be to tear the entire network infrastructure down and start over again from square one. In my idealized network protocol, which I will call the "No-Eavesdropping Data Transfer Protocol," or NEDTP, all connections would be point-to-point and determinative, meaning every device knows for an indisputable fact the identity of the other devices to which it is attached. No spoofing is possible. No man-in-the-middle attacks are possible. When a packet comes in, its origin and data integrity are assured by the simple expedient that every link along the way is known and any tampering modifies the integrity hash in an irreversible manner. This would suck from a privacy standpoint, but what we have now isn't exactly exemplary in that department. At least in my world you could buy crap online without needing your phone in the other hand to cancel that account when, moments later, the first inevitable fraudulent charge came through.

How easy would this be to implement? Beats me. I'm just the idea guy here. If I really had an unhackable network protocol, I'd be rubbing elbows with Elon Musk and having craters on Charon named after me. I'm just a humorist, after all. But I do know *something* needs to be done. I'm tired of getting emails and/or snail mail letters every other week announcing that yet another of the supposedly secure data archives to which my life's statistics are entrusted has been breached by hackers working for career criminals or the unfriendly state du jour. I have more free subscriptions to *LifeLock* these days than pairs of wearable shoes.

Maybe we should just stop *trying* to protect our vital information. If we all simply proceed on the presumption that every purchase, every bank account, every electronically enabled transaction of any sort is being monitored by criminals who fully intended to exploit whatever information we provide in order to conduct them, we might actually be safer. Instead of established account numbers, we could all use one-time pads that ceased to be of further utility the moment they were used. That pretty much describes all of my credit accounts, anyway.

I'd like to devote the rest of this column to addressing the thorny issue of operating systems, specifically the requirement thereof. Way back in the Cretaceous era of computing someone decided that just having a computer wasn't enough: it needed to be *usable* for something. So long as all users were engineers and deeply competent in machine language, the usability monster did not dare raise its misshapen head, but once the proposal was put forth that people who were not married to the system might want to do computing as well, the toxin-belching chimera was released into the wild.

It became obvious before long to those tasked with implementing this radical idea that some form of interface between the human who spoke a rich language full of nuance and complex syntactical rules and the machine that only made use of ones and zeroes was going to be needed. Various solutions were suggested to fulfill this requirement, the battles among the various camps reaching epic proportions at times. After much acrimony and several spoiled friendships, the basic operating system design that we know and love/loathe today emerged victorious.

What alternatives do we have to the familiar architecture? I, for one (because multiple personalities are so far not one of the mental aberrations with which I am saddled), would prefer that operating systems be stripped down. The examples we have today are so bloated with "features" that people spend huge chunks of their careers just trying to understand them. That's messed up, if you think about it. These are devices that are supposed to simplify our lives so we can devote more time and attention to the stuff that really matters, not occupy vast tracts of neocortical real estate in and of themselves.

Imagine needing a six-week course just to be able to make toast with your toaster. Ponder if you dare the impact of similar complexity on the efficient operation of your electric toothbrush. Except for those holding the Certified Powered Dental Cleansing Appliance Operator designation, we'd all be toothless.

I didn't intend to draw a parallel between operating systems and dental hygiene when I started out, but that's the nature of creative writing. Sometimes when you dig for gold you come across earthworms instead. When that happens it's time to go fishing.

I'll be out in the boat.