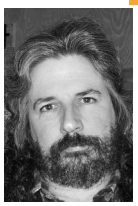
ROBERT G. FERRELL

# /dev/random: airport security and other myths



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

*rgferrell@gmail.com*

**I SPEND WAY MORE TIME THAN I WOULD** consider optimum sitting in airports these days. Admittedly, optimum for me would be a big fat goose egg, because I hate flying since the demise of the "friendly skies," so I suppose that really isn't a content-rich statement. Get used to it.

As an aside, I am typing this on my MacBook Pro, which I very much like except for the wonky keyboard. What possessed Apple to think that no one would miss the "Home," "End," "Page Up," and Page Down" keys? Sure, you can approximate those functions using keypress combos that take six or seven fingers like some insanely difficult guitar chord, but at my age digitary gymnastics of that sort are problematic. I guess Cupertino was aiming at a younger target market, although you'd think they would have mapped everything to thumb buttons and triggers in that case. I am half-expecting the next generation of input devices to be equipped with accelerometers that require you to go into three-dimensional spasms to send a text message or check the sports scores. At least that will be entertaining to watch, albeit hazardous for unwary passers-by.

It used to be that airport wireless access points were restricted to a few well-defined locations with somewhat limited coverage. With the advent of portable hotspots like the Overdrive, however, the network topology of the average airport is evolving rapidly. I can fire up KisMAC on the aforementioned trusty MacBook (bearing in mind that OS X is mostly BSD and therefore perfectly acceptable for use by us UNIX geeks) and as I walk from gate to gate the number of ad hoc networks that pop up is impressive. I happen to be slouching about at BWI at the moment, returning from scenic Linthicum, and because I'm the kind of guy who doesn't like to be rushed, I still have two full hours before my flight back to the sun-soaked South is due to depart. That leaves me plenty of time to conduct WiFi reconnaissance and to reflect on the current status of network security, a term frequently and wholly inappropriately applied to the chaotic lawless frontier that is the Internets.

There are a number of parallels between network security and airport security that I can see. For one thing, the growing horde of security "experts" who spent thousands of dollars and dozens of hours in some cheesy workshop memorizing the answers to an exam and are thereby qualified to secure the most complex rete of interconnected heterogeneous

systems ever conceived by sentient life (so far as we, the aforementioned sentients—and I employ the term generously—know) are eerily similar to the TSA. They provide a comforting illusion of competence and generate a warm fuzzy aura without providing any real security at all. It's pretty much just second-hand smoke and mirrors these days, whether you're boarding a 737 to Albuquerque or sending your credit card information over the Intertubes to a multibillion-taxpayer-dollar bailout recipient otherwise known as a bank. They won't let you bring a fingernail clipper on board an aircraft for fear you'll use it to overpower the flight attendants (by giving them killer manicures, presumably) and pry open the locked cockpit door with the little file, but apparently plastic explosives are OK so long as you tuck them in your underwear. If Semtex diapers aren't in your budget, just down a couple plates of the greasy bean and simulated cheese-like-substance–stuffed jalapeño appetizers at the restaurant across from your gate and you're good to go.

In the same vein, the little padlock that appears in your browser's status bar may be reassuring, but there's really not a lot of justification for that confidence. It means, ostensibly, that an encrypted SSL connection has been established with your remote host, but what it doesn't guarantee is that the remote host is who you think it is. Anyone with a valid certificate (which can be self-signed, by the way) can establish an SSL connection with you and, if they're clever, thoughtfully pass your information along to your intended destination after they get through with it, rendering the subterfuge very difficult to detect. This is called a "man-in-the-middle attack" by most of the industry, although I tend to refer to it as the "evil bucket brigade" because I'm not at all a well person. Call it what you will, it serves as yet another stark reminder of the illusory nature of security in an interconnected eSociety built on the confidentiality, integrity, and availability vacuum that is TCP/IP.

Returning to the airport security metaphor, let's talk about authentication. Having your boarding pass and driver's license available for TSA agents at the security checkpoint is sort of like authenticating, except that it's absurdly easy to circumvent. I love the way they shine the little light on your driver's license to give the impression they've been trained in how to spot clever forgeries for all fifty states, under the apparent assumption that no one but state governments has access to holographic printing. Even scarier, you can just go to work for one of the dozens of companies that provide support for the airport—many of whom conduct minimal background checks if any at all—and boom, you get to bypass even the rudimentary TSA butt-sniffing. While you're standing there getting probed, scanned, swabbed, and wanded, that guy in the coveralls driving the little catering truck with access to the delicate parts of the aircraft to which you are about to entrust your life may very well have a criminal record as long as the receipt for extra "fees" the airline has charged you in a desperate attempt to stave off the inevitable bankruptcy and or/merger looming in their future as their legacy of piss-poor business practices finally catches up with them. In infosec we refer to this as a "failure to apply discretionary access controls." In grammar we call it a "run-on sentence."

The airlines themselves could be considered system processes, and the gates I/O ports. That would make the terminals network segments, the trams connecting terminals bridging routers, your boarding pass the packet header, and you the actual payload. Despite what the airlines would like you to believe, air travel is definitely UDP. The encapsulation leaves much to be desired, as well. There's not even any error-checking to speak of, especially where baggage is concerned. If your packet fragments and fails to reach its

destination, the payload is irretrievably lost: resend isn't an option. Latency is also a serious problem. Collision avoidance, fortunately, is pretty robust, at least in controlled airspace when the pilots aren't busy playing FarmVille on their laptops. I must confess that I live in constant fear that my TTL will expire between hops.

In the final analysis, however, it seems to me that the information security term that best applies to airports these days is "denial of service."