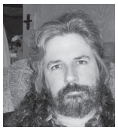
/dev/random

Cloud Control: Future (Mis)Directions for Information Security

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

A columnist of my ilk (A positive, with vitamin D and sodium benzoate added to prevent spoilage) realistically has only three basic choices of topic: what's going on with some aspect of technology now, what went on with some aspect of technology in the past, or what might happen with some aspect of technology in the future. I've churned out a fair amount of slush on the first two, so now it is time to offer my insights, such as they are, on what someday might have been.

Security is a crap shoot in the best of times, or maybe a roulette wheel. A roulette wheel fixed strongly in favor of the house; the house, as usual, being controlled by various unsavory elements (Sleazium, Larcenium, Felonium, et al.). Security is an abstract concept, unwieldy and unworkable in the real world. The bottom line is that where the rubber meets the road in the final analysis at the end of the day, "security" is overused and under-defined.

What we really mean when we talk about security is in fact "insecurity." A secure system is one that has not yet been designed and built; all secure systems are therefore future systems. Systems currently in operation, ipso facto, are inherently insecure, or at best both secure and insecure simultaneously. Taking the quantum superposition comparison further, any attempt to characterize the security of a system causes that duality to break down. Heisenberg would appreciate that you can never really calculate how secure your system is, only the probability that it has been compromised today. Or, for the purposes of this discussion, tomorrow. Security is Schrödinger's cat, long-deceased and skeletal.

Now that I've cleared some of the more egregiously tattered metaphors and dog-chewed aphorisms out of my virtual writing desk, I can relax and try to make some sense. The term "security" has, to paraphrase James Thurber, taken a terrific tossing-around in recent years and no longer means much of anything. There is no "security" in "information security;" there is only risk and the mitigation thereof. Risk management is where my professional attention is now directed because security is not something I know how to achieve. Those of you who are privy to the duties of my "day" job will understand. The rest can talk quietly amongst yourselves until the bell rings.

This trend toward increasingly draconian measures to self-identify to your software and hardware has just about reached its practical limitations, from what I can see. As Apple recently had the shattered pieces of its much-touted thumbprint authentication process for the iPhone 5S handed back to it in a paper bag by Germany's Chaos Computer Club, so will likely go most major "innovations" in access control for the foreseeable future. There is nothing you can possess, Dr. Jones, that I cannot emulate.

In my version of the future, authentication will move from the I/O device to the cloud. To authenticate, you tell the Master Interrogator Interface who you claim to be and three people you claim not to be. Once it verifies all four claims, you are granted access. That sounds perfectly potty, of course, but is it really any sillier than most other authentication protocols? I think not.

Maybe we'll see reliable whole-body photorecognition come into its own, as well. Those "selfies" you like to snap may someday get you access to your money or home entertainment/security system. Perhaps there will be a software photo mask that keys on a unique micro-attribute like your pore structure or acne scars.

Application security today is haphazard and depends mostly on programmers not making any of a dozen or so major blunders in their code: no bounds checking, relative paths, formatting errors, and so on. In the future, I predict that applications (which now reside solely in the cloud) will have no security measures at all taken during their coding. Because applications themselves will be modular with extreme granularity and distributed across the cloud, each instantiation of a particular program will be unique. Anti-malware functions will be provided by heuristically programmed agents in the cloud that watch for and forbid anomalous and/or dangerous behaviors. Antivirus companies will no longer sell subscriptions to signature files. Instead, they will activate their cloud heuristic agents for a set period of time for a specific customer . . . for the traditional hefty fee.

Thunderheads will be the airborne pathogens infesting the future cloud, much as Blackhats are the venomous spiders in today's Web. MITM will stand for "Man in the Miasma," because "middle" isn't very descriptive or accurate in a structure as amorphous as the cloud. Hackers will cease to have "handles" but will instead adopt "tail numbers." Being positively identified will be to "Fall Out" (of the cloud). Wags will call this "precipitation," but wags will always be wags.

Encryption, rather than referring to data scrambled by a complex algorithm that requires a lengthy key to reconstitute, will denote information that is actually en-crypted. That is, it will be encased in a cocoon built of layers of nonsense information that can only be penetrated and the data transcribed using the mathematical equivalent of a biological polymerase. Not only must the correct transcriptase be used, but the start and stop codons must also be correct—as must even the rate of transcription—or the message will not be comprehensible. Presuming, of course, it was comprehensible to begin with.

Web defacement, that exceptionally juvenile scourge of the late '90s and early '00s, will be replaced by attacks known as ODEs: On-the-fly Drive-by Exploits. As application code modules are assembled to order in the cloud, fragments of exploit code—able to hide from the heuristics agents by dint of being non-functional on their own—self-assemble into unique malware, the ultimate functionality and virulence of which depends on the identity and assembly order of the constituent fragments.

In closing, I'd like to stumble over Advanced Persistent Threats. I say "stumble over" because my favorite example of an APT is my cat. She's advanced—easily as smart as a toddler and much more creative; persistent—if she wants something, she is simply not to be ignored; and a threat—she's fond of sprawling across the narrow pathway I take every morning before dawn to get to my shower. But never in the same place twice. The fact that I have managed to remain fracture-free, proud to be, for 13 years as her roommate and food provider is nothing short of a miracle.

Thaumaturgy, coincidentally, is my candidate for the most robust information security tool available.