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

SEVERAL YEARS AGO, IN A FIT OF WHAT might best be described as literary bulimia, I disgorged a speculative fiction novel titled *Tangent*, that appellation being more a nod to my writing style than indicative of any deeply salient plot point foreshadowing. It was not a particularly good novel, even from my own healthy ego's perspective, and it was received, when received at all, with more negative comments than positive. Part of the problem, I think, is that it's really only the first part of a trilogy. I did put a fair amount of effort into creating a volume that would stand alone, but knowing the entirety of the plot makes it difficult, especially for a first-time novelist, to make sound decisions about how to slip in pointers to future plot lines while keeping those teasers ancillary to the conflict and resolution of the current story. One of the wholly unsolicited critiques a kind soul felt compelled to make, in a public forum, on reading *Tangent* was that it appeared to have been constructed using a series of ideas discarded by Neal Stephenson during the writing of *Cryptonomicon*. Now, despite the fact that I am a Stephenson fan, I had always been intimidated by the sheer bulk of that particular tome and so had not read it at the time my own foray into the commercial fiction world took place; thus this critical observation remains itself forever in the speculative fictional realm.

I now count myself among those lucky, if hardy, souls who have undertaken the odyssey presented by this monumental work (which I loved, by the way), and therefore I finally have a cogent response to the aforementioned accusation:

Huh?

First and foremost, encryption has nothing to do with *Tangent*. It's about quantum metaphysics, hacking, and duct tape. It reveals my staggering lack of knowledge concerning geography and airports in Great Britain and a narrative style that many might feel could well do with a good sound thrashing, but the relation it exhibits (at least as far as I can see) to anything covered, or to be accurate intentionally *not* covered, in *Cryptonomicon* could not be detected with even the most sensitive measurement device. Well, there are references to computers in both books.

Speaking of encryption, which of course is what prompted this little self-aggrandizing rant in the first place, I'm currently sitting on an MD-80 hurtling willy-nilly six miles above the Gulf of Mexico. In places like this a lot of the cultural fluff that ordinarily occupies my intellectual field of view is relegated to the musty stacks in the basement of my subconscious, there to fester like last week's discarded shrimp scampi. The fragrant vacuum this leaves is gradually filled by more esoteric cortical activities such as idle ruminations on the nature of cryptography.

Lest you fear I am now going to inundate you with elliptic curve arcana, be comforted by the fact that I don't understand that stuff very well. I can appreciate the elegance of the math the way a patron of the arts appreciates Van Gogh's energetic brush work, but trying it myself more often than not leads to numerical mayhem. In fact, my attempts at writing crypto algorithms have inadvertently created a whole new branch of mathematics I call "hermit theory" because they never go anywhere.

Cryptography is crazy stuff. A large number of very smart people have given a great deal of thought to creating ever more exotic processes for obfuscating human language. This wouldn't be quite so crazy except for the fact that human language is already about the most obfuscated means of communication imaginable. I think we could get some mileage out of melding the sciences of cryptology and molecular biology, though. Using DNA sequences for keys is hardly an original thought (although I did first think of it when I was in college in the 70s, so maybe it *is* original), but so far I don't see anyone doing it. Get with the program, people. While you're at it, where's my #@&! hoverboard?

One of the distinct inconveniences of encrypting communiqués is that for the result to be read by anyone, the intended recipient needs to have the same key (and complementary algorithm) used to encode them. This problem has been addressed in several novel and extremely clever ways, most notably PKI, with constantly increasing key lengths being one of the primary means of ratcheting up security as processing power continues its own inexorable advance.

I think it's time to think outside the packing crate here and come up with a new paradigm (I adore that word) using a radical form of key mechanism. Since we started off talking about Neal Stephenson, I'll borrow the kernel of an idea from him—for real this time—and suggest that we use subliminal memes based on person-specific cortical activity patterns as encoding keys. If you scan the message without the proper meme in place, it reads as gibberish. Since the interaction between a given person's neural cortex and the implanted meme will be unique to that individual, the odds that a computer could be used to replicate said key are absurdly remote, no matter the processing power involved. It wouldn't be a purely mathematical problem, for one thing, and computers don't yet deal well with the abstractions routinely taken in stride by the human brain.

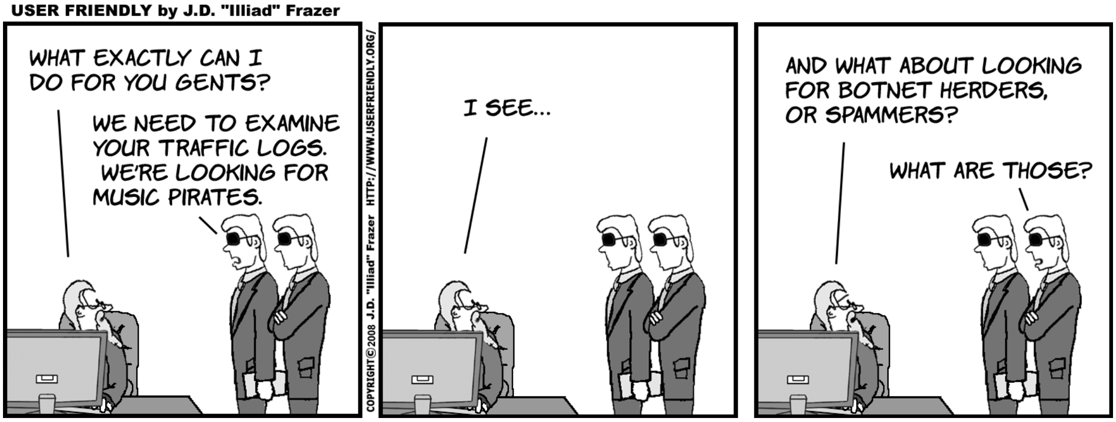
Implantation of the meme could take place using a device similar to the mind-erasing flashgun from *Men in Black*. The meme itself could be protected by a single-use safeguard, such that the implantation device will work once and only once, and would require a PIN or similar authentication to be activated. Any attempt to modify the device would render it permanently inoperable, like most of my cell phones. Thus, we have all the advantages of quantum cryptography without any of the logical contradictions.

Once the meme has been successfully implanted it is permanent, failing serious localized brain injury to the subject. The subject becomes, in effect, a living encryption key, able to decode encrypted messages merely by retyping them, as the neural processes involved in that mechanical act serve as the decryption mechanism.

If this sounds like far-fetched gobbledygook, consider quantum cryptography, the development of which is already well underway. In classical binary systems, the basic unit of information can have a value of 1 or 0. In a quantum system, the basic unit of information can have the value 1, 0, or *both*. That's what I call gobbledygook.

I've observed that the behavior of political candidates exhibits facets of all three systems: classical, relativistic, and quantum. The position a candidate takes on any given proposition is dependent on the observer (relativistic) and can be for, against, or both (quantum). Presidential candidates must belong to one of the two major parties in order to win (classical). American presidential politics, therefore, may well be the long-sought unifying theory of everything. The universe is composed neither of vibrating strings nor of oscillating toroids, but of annoying sound bites. Perhaps that should be sound *bytes*, given the pervasive nature of streaming audio/video.

Explains a lot, doesn't it? Do I really have to squeeze into a tuxedo to pick up the Nobel Prize, or will the dark suit I wear to weddings and funerals do?


USER FRIENDLY by J.D. "Illiad" Frazer
WHAT EXACTLY CAN I DO FOR YOU GENTS?
WE NEED TO EXAMINE YOUR TRAFFIC LOGS. WE'RE LOOKING FOR MUSIC PIRATES.
COPYRIGHT © 2008 J.D. "Illiad" Frazer HTTP://WWW.USERFRIENDLY.ORG/
I SEE...
AND WHAT ABOUT LOOKING FOR BOTNET HERDERS, OR SPAMMERS?
WHAT ARE THOSE?