/dev/random
Streamailer and Beyond

ROBERT G. FERRELL

Robert G. Ferrell is an award-winning author of humor, fantasy, and science fiction, most recently *The Tol Chronicles* (www.thetolchronicles.com).

I once regarded Snapchat as not much more than a novelty: interesting and well-intentioned, perhaps, but a novelty nonetheless. It seemed only a matter of time before an app or service invalidated the ephemeral nature of its content and therefore the sum total of its raison d'être. At the same moment, though, I thought perhaps having email that disappeared after a few minutes might be nice, too.

That led my fiction-writer's brain to pondering how spies could send one another short-lived messages by writing them out and taking pictures of them to be sent via Snapchat, or for more obscurity, embedding the message in said photos steganographically, thus giving the receiving party only a short time to decode them. I'm relatively certain this has already been done somewhere.

Getting back to the disappearing email idea, I was idly speculating one day (because energetic speculation has taken its toll on me over the years) that while I've tended to archive everything, there's really no need for this now. The vast majority of non-spam emails these days are just alternatives to text messaging; that is, they only convey information that is relevant for a comparatively short time.

The behavior this ephemeral nature drives, of course, is to delete mails as soon as you've read them, but this still leaves behind some artifacts in the form of temp files and "deleted email" boxes that presuppose you might want to "undelete" some of these from time to time. We've all deleted something we wish we hadn't at one point or another. But what if you're the type who sends messages you really, really don't want anyone but the recipient to see, ever?

My answer is Streamailer. In this killer app, every incoming mail is assigned a probability of being read according to its origin address information and subject matter. Mail messages stream constantly; you choose which ones to pluck out of the digital river. Messages from people you have marked as friends stream by more frequently, and are assigned to a different buffer. Others circle by only a set number of times if you don't actively delete them. The buffers are bit-complement overwritten at the end of each spool cycle. Not totally unrecoverable, but most people who might be snooping your personal business don't have a scanning tunnel electron microscope in their garage. At least, not one that actually works.

Moving on, it is time once again to poke at the squirming, slime-covered electric eel that is infosec. When I look out over the vast hysterical cybersecurity wasteland these days with the jaundiced eye of one who has retired from the field after many years of banging my head against any nearby hard surface as a result of the recalcitrant idiots I encountered, I have to chuckle. (I think I should get some sort of award for the preceding sentence.) What was back when I started in the 1980s an obscure IT subspecialty dismissed by most corporate and governmental honchos with the wave of an illegal Cuban cigar has now become an 800-pound gorilla sitting on the developed world's chest, beating its own and grunting loudly.

There is a certain satisfaction to be gained from having been one of a handful of information security people who can say "we told you this stuff was important 25 years ago," but it's attenuated by the fact that the associated excreta have impacted the ventilation system blades in a very big way. Identity theft, encryption munging, mobster-in-the-middle attacks, ransomware, spear-phishing...that litany of horrors makes Aleph's "Smashing the Stack for Fun and Profit" seem positively wholesome by comparison.

In 1994 I was working as the one-man IT department for a small-to-medium research company in Austin, Texas. I had been registering domain names for early Web adopters (my NIC handle was RGF4, to give you some idea of the time frame), and I had just accomplished same for my employer. I developed their first (text-based; hooray for Lynx) Web page, then added graphics to it when Mosaic was released. I had to create said graphics using MS Paint to build bitmaps pixel by pixel.

At that time I was administering a couple of Novell networks (50-node 3.11 and 3.12, if I recall correctly) for our internal data sharing. I had been using email on UNIX systems for over ten years by then, and I was aware of what a powerful and soon-to-be-ubiquitous communications medium it was. Once I had finally won the battle to register a domain name for us and develop a rudimentary Web presence, I started in trying to convince management that SMTP was the next logical step. I developed a PowerPoint presentation (yes, we had PP even back then) that showed all the nifty things we could accomplish if only we had email. He clutched the coiled wire-sporting handset of his beloved rotary dial desk phone with white knuckles and refused to consider my heretical proposal. SMTP, in his mind, could never hope to compete with POTS.

I did finally drag him into the email age, but it was a lengthy and exhausting battle. This same person, I should add, for years resisted any effort to install a network drop in his office. I would wire one in during the evening and the next morning he would put tape over it and order it removed. He was still using MS DOS 5 for all work as late as 1995. He would print out memos and have his secretary photocopy them for distribution. I half expected the mail room boy to come by and ask if I'd heard the new Frank Sinatra single.

If there truly is one, the moral underlying this little story is that it often requires a great deal of time, effort, and frustration to convince those in charge that they need to take action or change direction. I could point to the climate change debacle currently underway as another prime example of leaders who don't want to face up to an inconvenient reality, but I won't. Instead, I will finish up by abruptly changing the subject.

I have a new proposal for personal authentication. Instead of tired old passwords, security questions regarding your childhood best friend's favorite dog, and shining lasers up your nostrils, I submit that we should instead be using what I will call vocabulary profiles. Present people with recordings of a series of, say, ten words chosen randomly from a list. Ask them to spell each. The unique way in which a person (mis)spells ten relatively difficult words would make a decent identifier.

But why choose this method over any number of similar and equivalent ones? Because watching people misspell "misspelled" and "illiterate" is one of the little joys in the otherwise colorless life of a struggling novelist.