DOI:10.1145/3130331

Vinton G. Cerf

Take Two Aspirin and Call Me in the Morning

I use a lot of metaphors in this column and this one is about security. Security is much on my mind these days along with safety and privacy in an increasingly online,

programmed world. There is surely little doubt that we are at risk as cyber-attacks increase in scope, scale, and complexity. Our lives are made complex by some of the responses: “Oh, you want to log into this service? what’s your username and password? OK. Now go to your mobile to get a second password that I have sent you. You don’t have cell service where you are? Too bad.” I am *not* dissing two-factor authentication as I am a huge proponent, but I have experienced situations like this, or a dead battery and the frustrations are material. At that point, the system might turn to “answers to secret questions,” but that opens up the possibility that your choices of questions and answers are discoverable with a search of the World Wide Web. Ugh.

So where does this leave us? I am fascinated by the metaphor of cyber security as a public health problem. Our machines are infected and they are sometimes also contagious. Our reactions in the public health world involve inoculation and quarantine and we tolerate this because we recognize our health is at risk if other members of society fail to protect themselves from infection. Sadly, virus detection seems to be closing the barn door after the horses have left, to mangle a metaphor. Zero Day attacks cannot be detected with previously cataloged viral signatures, for example. They may help, but perhaps not enough.

One wonders whether we should take the metaphor more seriously and

quarantine computers showing signs of infection until they have been purged of their viral load? Of course, that raises the question “How do you know that computer or IOT device is infected?” and “How do you cleanse it?” Answering these questions might take you into potential privacy-violating territory: suppose your computer keeps track of every domain name and IP address it has interacted with. Could you use this list as a detector of potential hazard? Could you go to a service and say “Here’s where I have been—am I at risk?” Alternatively, you might download a blacklist of bad sites and addresses and compare to your list of places. We’ve seen some of the negative side effects of spam blacklists so I am not sure this would work, to say nothing of the question: “Quis custodiet ipsos custodes?”^a

I do wonder whether machine learning might be useful. Could my computer generate a profile of “normal” Internet interactions and warn me about unusual ones? Will the false alarm rate drive me crazy? How would I know if something is a false alarm? Is there anything like a center for disease control in this space? Google acquired a company called Virustotal^b a few years ago that maintains a library of viral profiles that allows users to check whether particular URLs or files carry malware. An-

other site, Stopbadware.org, helps infected websites rid themselves of viral load. There are, of course, a number of companies that offer anti-virus detection software that tries to detect malware as it is encountered or ingested into a computer. So far, these efforts have had only limited success and lead me to wonder whether there are more effective ways of discovering infection by way of behavioral observation.

It is tempting to imagine a home router/firewall that does sophisticated, machine-learned observation to protect programmable devices at home, but since our laptops, mobiles, and other programmed devices roam with us, they really need an on-board detection system (or logging system?) to protect while on the road.

Perhaps we all need to get into a cyber-hygiene habit and run our devices through regular infection checks? And we surely need much better tools with which to detect and combat this endless escalation. We could also do with better user training and services to avoid unsafe places on the Internet and poor security practices that lead to compromise. While I am not advocating for an Internet driver’s license, the preparation for such a metaphorical exam might do us all some good.

Vinton G. Cerf is vice president and Chief Internet Evangelist at Google. He served as ACM president from 2012–2014.

a Roughly, “Who will watch the watchmen?”

b <https://www.virustotal.com>