

Patch Grief with Proverbs

William Shakespeare, *Much Ado about Nothing*, Act 5, Scene 1

Immunity is advantageous. With immunity, you can operate fearlessly in the presence of noxious predators such as H1N1, anthrax, and prosecuting attorneys. Without immunity, your choices are (a) accept risk, (b) get immunized, and (c) avoid exposure.

are also largely scale-free, but at the cost of some institutions being “too big to fail.” (Sound familiar?)

In any case, what you’re looking for is “herd immunity,” which is when enough hosts are immune that the infection doesn’t spread. Taking R_0 as the number of secondary infections you get when you introduce a single infection into an unvaccinated population and R_v as the number of secondary infections you get when that population has been vaccinated, we have $R_v = R_0 \star (1 - C)$, where C is the coverage rate.

There will be no epidemic when $R_v < 1$, which is the same as $1 < R_0 \star (1 - C)$ —that is, there is no epidemic when $C < 1 - 1/R_0$. If, say, $R_0 = 2$, then 50% coverage is enough. On the other hand, if $R_0 = 100$, then 99% coverage is required. As you might guess, R_0 is heavily influenced by the number of contacts during the infectious period, so a promiscuous social network is a fertile ground for social diseases, whether medical or digital. Unsurprisingly, the black market for exploit tools is now focused on digital social networks.

There is much talk about immunization “in the factory.” In the medical sense, *in utero* vaccination is being studied variously. In the digital sense, the Build Security In development models are directly parallel. Even in agriculture we find this idea, where the genes conferring immunity to various pathogens are inserted into food crops, to the sorrow of some and the glee of others.

Of course, all this assumes that,



DANIEL E. GEER, JR.
In-Q-Tel

In the medical world, immunization is based on the body building resistance when it’s exposed to a non-lethal form of the infection. (“We” don’t create immunity; we just create the conditions in which it can be cultured.) In the digital world, immunization is based on injecting the immunizing agent directly, perhaps having built that agent by reversing an in-the-wild pathogen. In both the medical and the digital worlds, pathogenic mutation is evolution in action.

Detailed mathematical models of diseases are common in medicine but rare in digital security. The character of any worst-case infectious process is

- $\text{Pr}(\text{infection}|\text{exposure}) = 1.0$
- interval from infection to infectious = 0
- interval of infectiousness = open ended
- interval from infection to symptoms = indef
- duration of acquired immunity = 0 (mutates)
- non-lethal to carriers

By that definition, digital infections are almost always worst-case.

Choice (b) is immunization. Whether because of a scarcity of

labor, time, or vaccine, you can’t administer vaccine immediately to everyone. Priorities are required. In medicine, one strategy is to vaccinate against harm—babies and old folks go first—and the other is to vaccinate against transmission—primary and emergency medical personnel go first. As we’re writing this, US H1N1 vaccination prioritizes transmission. What would this look like in the digital world?

Patching against harm would target the most important machines first, which probably means according to a data value metric, given that data is a rising fraction of total corporate wealth. This does require knowing where your data is, however. Albert Barabási showed that a scale-free network is naturally immune to random faults (which is why the Internet works) but is completely vulnerable to targeted faults. This would indicate that patching against transmission might be the only choice because in a scale-free network, even weakly contagious infections both spread and persist.

Put differently, protecting data and protecting infrastructure have opposite immunization optimalities. Note that financial networks



DANIEL G. CONWAY
Augustana College


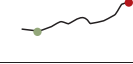
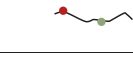
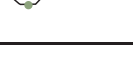

when we say “vaccine,” we mean a real vaccine that works. In the medical world, fake medicines including vaccines are available in more places than real ones are. In the digital world, fake anti-malware programs are for sale everywhere and far outnumber real anti-malware programs. (Symantec says 4×10^7 fakes are extant.)

Back to our initial triad—choice (c) is equivalent to quarantine. For those of you with the organizational authority, scanning your machines for a newly discovered vulnerability and then de-routing every machine that’s susceptible is a fine adjunct to forced patch-driven immunization. For those of you who are truly self-reliant, avoiding crowds, living clean, and experimenting with no unknown substances is as much an immunization procedure in the digital sphere as it is in the physiologic.

Arbor, Symantec, and SecureWorks have reported drops in underground prices and increases in active bot-infected computers (up over 30% from the previous year). They offer increased supply and lower barriers to entry as the reason for the price drops. The drop in DDoS prices alone lowers the ØPI by US\$3,500. The other components of the ØPI remain unchanged from the last issue, though we’ve noticed other signs of economic maturity, including quality-of-service guarantees (Remote Desktop 24-hour availability guarantee) and discriminate pricing (declined credit-card accounts for 1/20 the price of active accounts). Also, some vendors are offering “how-to” services along with their products (learn how to spam: \$40 if you purchase the email list). Next issue, the ØPI

will be updated to reflect market activity in social networks, but as of the end of October, it stands at \$63,279.60.

At the same time, our Security Pressure Index continues to ramp upward (bad):

INDEX	PREVIOUS	CURRENT	TREND
Phishing	476	662	
Spam	299	312	
Workfactor	112	92	
Dataloss	150	153	
Composite SPI	259	305	

Daniel E. Geer Jr. is the chief information security officer for In-Q-Tel. He was formerly vice president and chief scientist at Verdasys, and is a past president of the Usenix Association. Contact him at dan@geer.org.

Daniel G. Conway is an associate professor of business administration at Augustana College. He previously served on the faculty at Indiana University and the University of Notre Dame. Contact him at danielconway@augustana.edu.



Silver Bullet Security Podcast

In-depth interviews with security gurus. Hosted by Gary McGraw.

www.computer.org/security/podcasts

Sponsored by 