The Future of Security

Criticality, Rejectionists, Risk Tolerance

DANIEL E. GEER, JR.

Dan Geer is the CISO at In-Q-Tel and likes to list the following milestones: the X Window System and Kerberos (1988), the first information security consulting firm on Wall Street (1992), convenor of the first academic conference on electronic commerce (1995), the "Risk Management Is Where the Money Is" speech that changed the focus of security (1998), the Presidency of the USENIX Association (2000), the first call for the eclipse of authentication by accountability (2002), principal author of and spokesman for "Cyberinsecurity: The Cost of Monopoly" (2003), co-founder of SecurityMetrics.Org (2004), convener of MetriCon (2006–present), author of "Economics & Strategies of Data Security" (2008), and author of "Cybersecurity & National Policy" (2010). Creator of the Index of Cyber Security (2011) and the Cyber Security Decision Market (2011). Six times entrepreneur. Five times before Congress.
dan@geer.org

Pew reports [1] that

One in five American adults does not use the Internet. . . . Among adults who do not use the Internet, almost half [said] that the main reason they don't go online is because they don't think the Internet is relevant to them. . . . Though overall Internet adoption rates have leveled off, adults who are already online are doing more.

It may no longer be possible to live your life without dependence on the Internet. Unlike television, you cannot entirely unplug from the Internet even if you want to. If you are dependent on those who are dependent on television, then so what? If, however, you are dependent on those who are dependent on the Internet, then so are you. Dependence with respect to television is not transitive. Dependence with respect to the Internet is.

The source of risk is dependence, and security is the absence of unmitigatable surprise. It is thus obvious that increasing dependence means ever more difficulty in crafting mitigations, and that increasing complexity embeds dependencies in ways such that while surprises may grow less frequent, they will be all the more unexpected when they do come.

Because dependence on the Internet is transitive, those who choose "leave it" with respect to the Internet only get to say that in the first person; they are still dependent on it unless they are living a pre-industrial life. That rejectionists depend on people who are not rejectionist is simply a fact. Everyone has a stake in the game, but rejectionists have impact on the Internet-happy—rejectionists are now a kind of fail-safe. If we begin to penalize the rejectionists, that is to say, force them to give up on their rejectionism, we will give up a residuum of societal resiliency.

On November 13, 2002, a total computer outage at Boston's Beth Israel Hospital began [2]. The initiator was inadvertent high volume of data sharing among researchers; the impact was reverting to paper for four days, during which time doctors and laboratory personnel over 50 years old could cope; most of the rest could not. That a fallback to manual systems was possible saved the day, and it was those who could comfortably work without network dependence who delivered on that possibility, because they had done so at earlier times.

Thus the central thesis of this essay: accommodating rejectionists preserves alternate, less complex, more durable means and therefore bounds dependence. Bounding dependence is the core of rational risk management.

Common mode failure comes from under-appreciated mutual dependence. In NIST's High Integrity Software System Assurance documentation [3], they say, "A more insidious source of common-mode failures is a design fault that causes redundant copies of the same software process to fail under identical conditions." This is exactly what can be masked by complexity precisely because complexity ensures under-appreciated mutual dependence.

In an Internet crowded with important daily-life functions, the possibility of common-mode failure is no idle worry. The Obama administration is notably increasing dependence on the Internet on two fronts, either of which might be said to be, in the words of President Clinton's Presidential Decision Directive 63, "essential to the minimum operations of the economy and government": the press for electronic health records, and the press for the Smart Grid.

Electronic health records depend on the smooth functioning of electric power, networks, computers, displays, and a range of security features [4]. The Smart Grid depends on good clocks, industrial controls operated flawlessly at a distance and guaranteed not to lie about their state, and another range of security features.

Both of these involve new levels of exposure to common-mode risk; both add new failure modes to the world we live in. On good days, both will deliver cost-effective benefits. On bad days, doing without those benefits will be easier for those who can remember not having had them.

Each new dependence raises the magnitude of downside risk, the potential for collateral damage, and the exposure of inter-relationships never before contemplated. Forget the banks: it is the Internet that is too big to fail. While there is no entity that can bail out the Internet, there is no meaningful country that is not developing ways to disrupt the Internet use of its potential adversaries.

When 10% of the population sees nothing in the Internet for them, should we respect and ensure that, as with the Amish, there is a way for them to opt out without choosing to live in a cave? Should we preserve manual means?

I say "YES" and I say so because the preservation of manual means is a guarantee of a fallback that does not have a common-mode failure with the rest of the interconnected, mutually vulnerable Internet world. That this is not an easy choice is an understatement. I do not (yet) claim to have a fully working model here, but neither do our physicist friends (yet) have a unified field theory.

Summing up, risk is a consequence of dependence. Aggregate societal dependence on the Internet is not estimable. When dependencies are not estimable, they are underestimated. If they are underestimated, they will not be made secure over the long run, only over the short. As risks become increasingly unlikely to appear, the interval between events will grow longer. As the latency between events grows, the assumption that safety has been achieved will also grow, thus accelerating dependence in what is now a positive feedback loop. If the critical infrastructures are those physical and cyber-based systems essential to the minimum operations of the economy and government [5], and if aggregate risk is growing steadily [6], then do we put more of our collective power behind forcing security improvements that will be sharply diseconomic, or do we preserve fallbacks of various sorts in anticipation of events that become harder to mitigate as time passes? Is centralizing authority the answer, or is avoiding further dependence until we can fix things the better strategy? Should the individual who still prefers to fix things he

or she already has be celebrated, or are those individuals to be herded into National Health Information Networks, Smart Grids, and cars that drive themselves?

Resources

[1] "Digital Differences," Pew Research Center, April 13, 2012: http://pewinternet.org/~/media//Files/Reports/2012/PIP_Digital_differences_041312.pdf; tinyurl.com/d7eqo7v.

[2] P. Kilbridge, "Computer Crash—Lessons from a System Failure," *New England Journal of Medicine*, vol. 348, no. 10, 6 March 6, 2003, pp. 881-882: http://ehealthecon.hsinetwork.com/NEJM_downtime_2003-03-06.pdf; tinyurl.com/75fjmbb .

[3] NIST, High Integrity Software System Assurance, section 4.2: http://hissa.nist.gov/chissa/SEI_Framework/framework_16.html; tinyurl.com/canwggd.

[4] Simon S.Y. Shim, "The CAP Theorem's Growing Impact," *IEEE Computer*, vol. 45, no. 2, February 2012, pp. 21–22.

[5] Presidential Decision Directive 63, May 22, 1998, http://www.fas.org/irp/offdocs/paper598.htm; tinyurl.com/4974j.

[6] The Index of Cyber Security: http://cybersecurityindex.org.

This article was abridged by the author from his keynote address for the Rocky Mountain Information Security Conference, Denver, May 17, 2012, which can be found at www.usenix.org/publications/login/august-2012/future-security.