For Good Measure

Stress Analysis

DAN GEER

Dan Geer is the CISO for In-Q-Tel and a security researcher with a quantitative bent. He has a long history with the USENIX Association, including officer positions, program committees, etc. dan@geer.org

> Reality is the leading cause of stress amongst those in touch with it.
>
> —Jane Wagner

In retrospect, the financial collapse of 2008 had useful side effects. We in distributed computing can be rightly thankful that it was the financial services world that shouldered the task of proving that (we) humans are in fact entirely capable of building systems that (we) humans cannot then understand well enough to stably operate. I say thankful as (1) it wasn't us, and (2) money lost can be replaced with money printed, but not everything is so fungible.

One of the useful side effects was that of ratcheting up the compulsory simulations of bad events. Various sovereigns require these; most are called "stress tests." What these stress tests propose to do is to show how the largest bank holding companies (BHCs) would fare in the event of various unhappy financial events in general, things that are "shocks to the system" for which the BHC must either be able to absorb or be invulnerable to the contagion.

I've long considered financial services to be the avatars in cybersecurity simply because the financial world differs from every other industrial sector in that the bigger the bank, the greater the percentage of its business is done with competitors (i.e., BHCs are mutually dependent). I'm here to suggest that it is that mutual dependence that generates risk of the sort that stress tests exist to measure.

In another column long ago, I tried to explore the idea of a "margin of safety" for cybersecurity, something on par with how a civil engineer thinks about bridge failure under load. Cryptography has long had such concepts. I now think that the stress test route is the one for cybersecurity to follow. In a way, some already do this—including contingency plans for data breaches that involve reverting to paper while evidence is gathered [1].

We all know that organized crime and military powers alike have both tools for mass disruption and tools for precision targeting. With that said, the pervasive interdependence of the current Internet sphere is certainly on par with the interdependence of financial markets. The time constants (speed) of the exchange of data and control between major cyber-infrastructures are smaller (faster) than everything else on the planet excepting, perhaps, financial services engaged in high-frequency trading.

So the obvious question is what sorts of simulations might be appropriate metrics for assessing public risk to private yet critical components of the Internet ecosystem? And to whom might a requirement for cybersecurity stress testing apply? As to the latter, in finance the stress tests are required of "systemically important financial institutions" (SIFIs), which include not only banks but also insurance companies and market infrastructure providers [2].

As to the question of what simulations and cybersecurity metrics might be appropriate, in finance the scenario for 2012 stress testing [3] was

- a peak unemployment rate of 13 percent,
- a 50 percent drop in equity prices, and
- a 21 percent decline in housing prices.

If applying such scenarios to major financial institutions represents our best available analogy for what to do in cybersecurity, then how can we in cybersecurity proceed?

The cybersecurity equivalent of the SIFI would include the most important transport providers (ISPs), cybersecurity product suppliers, identity providers, intelligence acquirers and analysts, and any of the XYZ-as-a-service suppliers as have clients who are themselves critical infrastructure players and for which security is part of the claimed package of service benefits. It is likely that in cybersecurity we'd have a longer list than the eight domestic and 32 global SIFIs, because for finance it is easy to tell who to include by the "too big to fail" test, whereas for cybersecurity the web of dependencies is more like looking for those entities that are "too interconnected to fail."

The cybersecurity equivalent of the stress test would not be just one scenario but, rather, a number of scenarios. Let me suggest, however, one sample parallel to that which is applied to the SIFIs, viz., the simultaneous appearance of

- a vulnerability requiring client-side reinstallation for 25 percent of all endpoints,
- a sustained 50 percent drop in available bandwidth, and
- the wholesale data loss of a top-three cloud provider.

As with the banks, the question is whether the enterprise being stress tested can survive in the above scenario. Stress tests are fundamentally different from the tests (and associated metrics) that come from such disparate things as static analysis of code, penetration testing, cryptographic strength assessment, and so forth. In every case with which I am familiar, the tests we currently do are designed to answer the question, "Am I or my clients at risk from things that I am supposed to directly control?" The tests I am proposing answer a different question: "Can I withstand the failure of others on whom I depend?" That gets to the very heart of risk—a dependence on the expectation of system state.

I would like to work with a number of interested parties to come up with a set of scenarios, a set motivated by the systemic risk to those other entities that depend on the cybersecurity industry and which would ask questions in the same spirit that the stress tests mandated by Basel III [4], Dodd-Frank [5], the European Banking Authority [6], and so forth, ask: Can the institutions be made to survive cyber-failure scenarios through the application of cybersecurity techniques that we already have in hand, or not?

The stress testing of financial institutions could not have come into force without the near approach of general collapse on a global scale. Must we hope for the near approach of general collapse on a global scale within the cybersecurity infrastructure? One wishes otherwise, but if such a crisis does occur, then we cannot let it go to waste. Thinking and writing about what a useful cybersecurity stress test regime would contain is the best way to avoid letting the coming crisis go to waste. With the possible exception of finance, no part of modern life offers the chance of common mode failure as much as cybersecurity does [7]. It is our duty to realistically measure that risk and to prepare or preserve alternate paths. Finance has, unwillingly or no, blazed a trail. What will we do?

References

[1] US restaurant chain P.F. Chang's China Bistro reverted to manual credit card imprinting during investigation of a security breach that allowed hackers to steal customer payment card data from multiple stores: arstechnica.com/security/2014/06/pf-chang-turns-to- vintage-1970s-tech-after-credit-card-breach/.

[2] "List of systemically important banks," Wikipedia: en.wikipedia.org/wiki/List_of_systemically_important_banks.

[3] Federal Reserve Board of Governors, Comprehensive Capital Analysis and Review: www.federalreserve.gov/newsevents/press/bcreg/20120313a.htm.

[4] Bank for International Settlements, International Regulatory Framework for Banks(Basel III): www.bis.org/bcbs/basel3.htm.

[5] US Senate Committee on Banking, Housing, & Urban Affairs, Brief Summary of Dodd-Frank Wall Street Reform and Consumer Protection Act: www.banking.senate.gov/public/_files/070110_Dodd_Frank_Wall_Street_Reform_comprehensive_summary_Final.pdf.

[6] European Banking Authority, EU-wide stress testing: www.eba.europa.eu/risk-analysis-and-data/eu-wide-stress-testing.

[7] Dan Geer, "Heartbleed as Metaphor," *Lawfare*, April 21, 2014: www.lawfareblog.com/2014/04/heartbleed-as-metaphor.