Cybersecurity in 2025: Is there a Case for Optimism?

Lee Badger
NIST

Should we be optimistic about cybersecurity, either today or in the future? The combination of increasing software complexity, increasing network connectivity, a user community ranging from innocent neophytes to state-sponsored threat actors, and increasing reliance on flawed software throughout society presents ample cause for concern.

The recent Heartbleed OpenSSL vulnerability illustrates the essential brittleness of cybersecurity today: a few statements in server-side code trusted a client provided value (payload) and the (otherwise correct) server-side statement

memcpy(bp, p1, payload); [1]

then could be controlled by malicious clients to copy up to 64k of possibly sensitive server memory, leaving virtually no trace. Because of the heavy reliance on this code, the cybersecurity damage may be extensive and will likely never be quantified.

It is important to understand that this kind of error is very common and is hard to entirely avoid; e.g., the National Vulnerability Database (nvd.nist.gov) shows over 2,600 *reported* disclosure-impacting flaws across numerous software packages. It is likely that many, many more are undiscovered or known-but-unreported. And, of course, that is considering just *one* kind of cybersecurity problem among many.

Will we do better, perhaps over the next 10 years? Current ideas like Cloud Computing or Big Data or the Internet of Things may affect cybersecurity brittleness for better or worse. 10 years is a long time and today's ideas may by then seem a bit quaint.

Nevertheless, I would like to suggest that, in the longer term, there are several bases for optimism.

Richer Programming Languages and Programming Environments. Higher-level languages and development "wizards" may reduce the production of low-hanging vulnerabilities.

Increasingly Mature Domain-Specific Frameworks. Re-use of well-tested code may increase.

Additive Software Analysis Techniques. An increasing set of problematic and virtuous programming patterns and idioms may be checkable by tools.

Research Innovation. Attackers don't always win. Particularly in research settings, the combination of layered defenses, replication, and software diversity has performed well against red team attackers, but at a cost. Continued research innovation is, I think, our best defense as threats continue to evolve.

These bases, among others, give me hope that we can make significant progress by 2025. By then, my hope is that high-reliance software will be (mostly) composed from well-analyzed components, and will have very low exploitable flaw densities; failures will still happen, but less frequently, and with more measurable effects.

---

[1] Code from the Jan. 6 version of t1_lib.c at www.openssl.org.