Why is cybersecurity so bad

&

What can we do about it

International Federation for Information Processing (IFIP) Working Group 10.4
on
Dependable Computing and Fault Tolerance

86th Meeting
Saint Simon's Island
Georgia, USA

Jaynarayan H Lala
Senior Principal Technical Fellow
Raytheon, an RTX Business

jay.lala@rtx.com

4 February 2024

The views expressed in this report do not necessarily reflect those of the author's affiliation.

ifip

WG 10.4

In this “Research Report,” I want to address the topic of cybersecurity, specifically, why is it so bad and what can we do about it.

We, as a community, have been working on cyber resiliency for over a quarter century. Yet, there is almost a constant daily drumbeat of cyber incidents, from minor ransomware annoyances to serious financial fraud, massive identity theft, intellectual property theft at vast scale, penetration of important private and government institutions, election interference, spying and other national security incidences.

By contrast, about a quarter century after the community started addressing hardware, software, and operator faults, errors, and failures, the discipline had matured to the point of offering practical and affordable solutions. Fault-tolerant and dependable systems were widely deployed in all parts of society, including, finance, transportation, manufacturing, industrial control systems, and even the most demanding safety-critical systems such as automated train controls and aircraft fly-by-wire flight control.

In my opinion, there are two reasons for this disparity in the pace of progress of two disciplines: 1) Governance, and 2) Technical.

In both cases, our solutions are incomplete, and approaches are stale and dated. Both areas need innovation.

Governance

The fundamental difference between traditional fault-tolerance and cybersecurity is that a cyber attack is a crime. But we have been, for the most part, focused on technical solutions. That is necessary but not sufficient to counter criminal behavior.

What we need is a “whole of society” approach. While there are some laws against hacking in many countries, they are not comprehensive and do not address the constantly evolving cyber threats. Very few cyber criminals are caught and even fewer are prosecuted. Punishment is light, partly because of the societal perception of these crimes as not being violent, with no physical harm to people or property.

Furthermore, cyberspace transcends national borders. Bad actors can very easily reach across national boundaries to commit crimes. They maybe hard to geolocate and extradite. Some nations knowingly harbor them and provide indirect protection. Then there are the nation-states themselves which engage in cyber warfare without an explicit declaration of war.

International treaties, cyber laws, mutual understanding on tacit limits on peacetime cyber warfare, and active cooperation and collaboration between relevant agencies of friendly countries (law enforcement, intelligence, defense) are needed to address the boundaryless dimension of cybersecurity.

Again, much work is being done in all these areas in the US as outlined by National Cybersecurity Strategy. But, more resources, proportional to the threat that is constantly increasing, need to be marshalled.

In addition to finding, prosecuting, and punishing cyber attackers, the companies that provide products and services that get hacked, must also be held accountable.

Carl Landwehr suggested, during Session 3 discussion, that there ought to be liability for any company whose products do not meet some minimum security standards. Cristina mentioned that the credit rating agency, Equifax, did not suffer any consequences when criminals exfiltrated personally identifiable information (PII) of nearly 140 million Americans. The only penalty, it appears, was for them to pay for a year worth of credit monitoring services to those victims who bothered to enroll.

Reaching consensus on what the minimum standards is a challenge that spans technical, law, government regulatory policies, and business dimensions. Then there is the issue of what penalties must be assessed when cyber-deficient products and services are hacked. There are many other defective products, from consumer items to automobiles to airplanes for which these challenges have been successfully addressed. They could serve as a template for the cybersecurity domain.

The cybersecurity technical community, in the meantime, is more or less working in a parallel universe that's not engaged with the rest of society's non-technical thrusts. Perhaps a better awareness of each other's efforts as well as some coordination of their approaches, may result in a more effective approach to combat cyber threat.

Technical

On the technical front, the mindset has not changed in the past quarter century. It's all about building higher forts and deeper moats. These defense mechanisms are essential to prevent simpler threats from unsophisticated hackers, known as "ankle biters." But they fail to keep out determined and goal-oriented sophisticated attackers, especially well-resourced nation-state actors who can and do penetrate multi-layered defenses. Then the tactic shifts to intrusion detection. But the game seems to just stop there.

This is an incomplete solution. What's missing is everything that needs to be done after an inevitable successful intrusion: damage containment, repair, recovery, and continued operation. When taken together, we can call this response intrusion tolerance. The very first program I formulated at DARPA in 1999 was called Intrusion Tolerant Systems (ITS). It was focused on developing the fundamental concepts of systems that can continue to operate correctly, maybe with some graceful degradation in functionality, even when successfully penetrated.

Mission- and safety-critical systems cannot be disconnected and turned off when an intrusion is detected. Critical systems in finance, transportation, healthcare, aerospace, defense, industrial control, etc. must continue to operate the critical core functions without interruption even when some part of the system may have been compromised. The bumper sticker for DARPA's ITS program was "Operate Thru' Attack." This is a paradigm that has been adopted by the US Dept of Defense as a policy, designated as "Cyber Survivability."

Unfortunately, most research as well as new cybersecurity products continue the old and dated paradigm of prevention and detection.

In addition to intrusion tolerance concepts, architectures, and techniques, we also need to treat cybersecurity as another front in war. Over a hundred nations have offensive cyberwar initiatives.

To approach cybersecurity with the mindset of fighting a war, we need to add technical capabilities to help fight this war in cyberspace. We can adapt these capabilities, at the conceptual level, from kinetic war. Fighting a war with tanks, troops, missiles, ships, and airplanes requires Battle Management and Command and Control to direct the overall battles. These have many components. Some of the functions relevant to cyber warfare include (cyber) threat intelligence, (cyber) battle plans, (cyber) maneuvers, and rapid decision making at tactical, operational, and strategic levels. While kinetic analogs are helpful, we need to translate these into relevant cyber concepts, architectures, plans, and actions.