Rethinking general-purpose computing—toward an internet of secure things

January 19 2017

In the 1930s Alan Turing imagined a "universal computing machine" capable of computing nearly anything. Today, that universality is the backbone of the information age: Turing-like computers are running governments, businesses, homes, power grids, vehicles, and cities, all

linked by a scaffolding of common hardware, software, and network protocols.

But Turing did not foresee the security threat that arises from this universality: with a few bits of cleverly designed code, a malicious actor can take over a system and execute an attack never envisioned by the system's designers. The result is a cyber arms race in which attackers and defenders invent increasingly effectives means to thwart the other.

Might fundamental changes in hardware or software architectures shift the balance of this race? Opening that conversation was the chief goal of a recent two-day working group, "Circumventing Turing's Achilles Heel," held in Santa Fe.

"It all comes down to the asymmetric nature of the problem," says SFI External Professor Chris Wood, who organized the meeting. "The attacker needs only one 'weak link'—one vulnerability—to be successful, whereas the defender must successfully anticipate and defend every vulnerability, in every element of the system, all the time."

Participants in the November meeting included experts from industry, government, and academia representing computer science, hardware and software engineering, and cyber security. Much of the discussion focused on reviewing the state of the art, science, and engineering on both theoretical and practical fronts, as well as public and private priorities for future progress.

It is clear, says Wood, that government and industry are paying increasing attention to cyber security. But it is also clear that most such efforts are examples of "cyber-security-as-usual," he says, in which "attackers identify new vulnerabilities, defenders devise means to detect and mitigate them, and so on."

The meeting focused on two possible directions for fundamentally reframing the problem: The first, termed "formal methods," uses logical or mathematical descriptions of computer hardware and software systems to produce provable models and verifications of computer behavior, so cyber defenders can be sure their systems execute only as intended.

The second, termed "executable space protection," uses hardware strategies to keep certain areas of memory "unwriteable" to prevent execution of unintended code, thereby making attacks more difficult.

"We succeeded in establishing a basis for a productive discussion across disciplinary boundaries that recognizes the big differences between government, industry, and academia," Wood says.

The group plans to continue the exploration of novel approaches in future meetings.

Provided by Santa Fe Institute