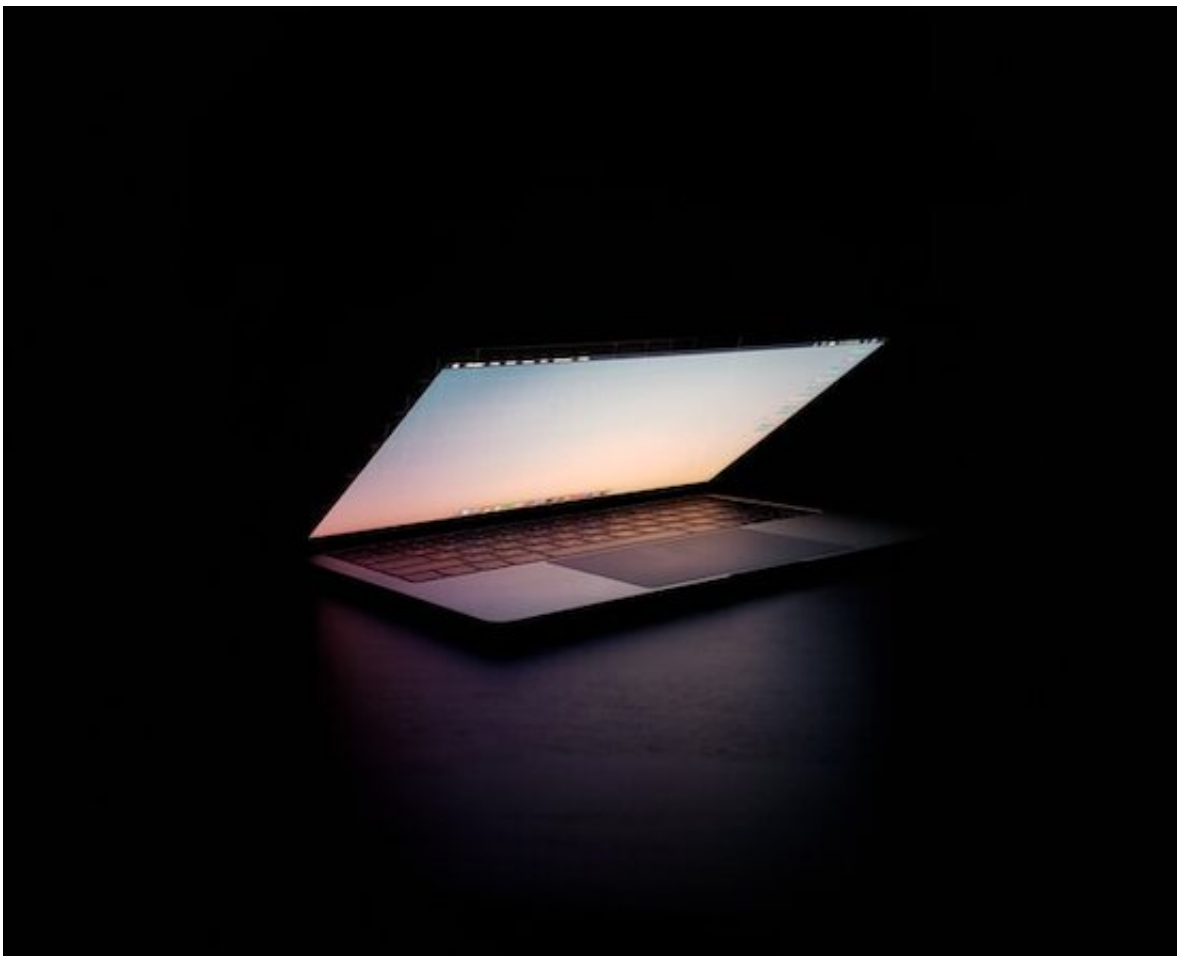
Researchers reveal a new computing platform that is provably secure even alongside software compromised I/O devices

June 15 2021, by Daniel Tkacik



Credit: Carnegie Mellon University

The trek towards the holy grail of cybersecurity—a user-friendly computing environment where the guarantee of security is as strong as a mathematical proof—is making big strides.

A team of Carnegie Mellon University CyLab researchers just revealed a new provably secure computing environment that protects users' communication with their devices, such as keyboard, mouse, or display, from all other compromised operating system and application software and other devices. That means that even if malicious hackers compromise operating systems and other applications, this secure environment is protected; "sniffing" users' keystrokes, capturing confidential screen output, stealing or modifying data stored on user-pluggable devices for example, is impossible.

"In contrast to our platform, most existing endpoint-security tools such as antivirus or firewalls offer only limited protection against powerful cyberattacks," says CyLab's Virgil Gligor, a professor of electrical and computer engineering (ECE) and a co-author of the work. "None of them achieve the high assurance of our platform. Protection like this has not been possible to date."

The groundbreaking work was presented by Miao Yu, a postdoctoral researcher in ECE and the team's lead implementor, at last month's IEEE Symposium on Security and Privacy, the world's oldest and most prestigious security and privacy symposium.

Specifically, the researchers presented an I/O separation model, which defines precisely what it means to protect the communications of isolated applications running on frequently compromised operating systems such as Windows, Linux, or MacOS. According to the researchers, the I/O model is the first mathematically-proven model that achieves communication separation for all types of I/O hardware and I/O kernels, the programs that facilitate interactions between software and

hardware components.

Imagine that you need to transfer some money online, and the transactions you are about to execute are so sensitive that you'd like a guarantee they will remain private even if your computer has unknowingly been compromised with malware. Performing those transactions in this environment would be provably secure; even your completely compromised operating system would be unable to steal or modify the private data you input using your keyboard or mouse and display on your screen.

This type of secure environment is even more important with the rise of remote work, as more and more workers are utilizing Virtual Desktop Infrastructures (VDIs) which allows them to operate remote desktops.

"Business, government, and industry can benefit from using this platform and its VDI application because of the steady and permanent shift to remote work and the need to protect sensitive applications from future attacks," says Gligor. "Consumers can also benefit from adopting this platform and its VDI clients to secure access banking and investment accounts, perform provably secure e-commerce transactions, and protect digital currency."

This platform is still in the development phase, but Gligor and his team aim to commercialize it in the coming years.

More information: An I/O Separation Model for Formal Verification of Kernel ImplementationsOpens in new window, www.computer.org/csdl/proceedi … 3400b746/1t0x9DPKE36

Provided by Carnegie Mellon University