Phoenix Partners With Rutkowska in Securing Hypervisor

New ultra-thin hypervisor will benefit from further Blue Pill research

OCTOBER 25, 2007 | 5:08 PM

By Kelly Jackson Higgins
Senior Editor, *Dark Reading*

Phoenix Technologies has teamed up with researcher and stealth malware expert Joanna Rutkowska and her company, Invisible Things Lab, to help secure an ultra-thin hypervisor that the firmware company is currently building. The company also plans to support further development of Rutkowska's famed Blue Pill virtualized rootkit prototype -- for thin hypervisor research. (See Blue Pill Gets a Refill.)

Rutkowska, founder of Invisible Things Lab, says the problem with most hypervisors today is that they are too large, which leaves them open to complexity, and therefore, vulnerabilities. "We should make sure our VMMs (hypervisors) are as thin as possible. Today, that's not the case. They're too big, almost like conventional OSes," she says.

Phoenix's new, slimmed-down hypervisor technology aims to make that footprint smaller, and will run embedded operating systems within its virtual machines. According to a Phoenix slide presentation to investors, the hypervisor's architecture is resistant to rootkits.

The first iteration of HyperCore will provide two operating systems -- one Vista-like OS and another small, custom, secure OS developed by Phoenix, according to Rutkowska.

"The user will be able to switch between those OSes on the fly, using special key combination," she says. That way, a user could use the hardened, smaller OS to do online banking transactions, for instance, she says.

Phoenix officials declined to comment on the as-yet unannounced product.

"Phoenix is in a unique position -- they are one of the biggest BIOS providers for all those PCs around the world," Rutkowska says. "The HyperCore hypervisor will be loaded from within BIOS, before any other OS. This gives unprecedented possibilities, both from a security and a usability point of view."

And Phoenix plans to leverage Invisible Things Lab's Blue Pill technology. "Phoenix would like to use our experience with thin hypervisors -- Blue Pill is a very thin hypervisor -- to make sure that their product will be secure and effective," Rutkowska says.

Rutkowska says Phoenix will support further research on Blue Pill, and will use it as a testbed for trying out new features for HyperCore, such as so-called "nested" virtualization (think Blue Pill within a Blue Pill). (See Blue Pill Gets a Refill and Hacker Smackdown.)

"Blue Pill should be understood as a research project into virtualization technology, not malware," she says. "Malware is just one application."

Rutkowska, who will speak at the upcoming SecTor security conference in Toronto, expects the new Blue Pill research, including code, to be made available to other researchers.

Have a comment on this story? Please click "Discuss" below. If you'd like to contact Dark Reading's editors directly, send us a message.

- Phoenix Technologies Ltd. (Nasdaq: PTEC - message board)
- Invisible Things Lab