Defending your computer from cyber-attacks, Sun Tzu style

January 21 2016, by Alisson Clark

We want our computers to perform the way we expect. But what if the key to defeating malware is introducing a bit of chaos?

Daniela Oliveira, a professor in the University of Florida Herbert Wertheim College of Engineering, thinks a bit of unpredictability could help outsmart malware. That's the logic behind Chameleon, the operating system she's developing with colleagues at UF, Stony Brook University and the University of California, Davis.

In Chameleon, which is still at the conceptual phase, unknown programs that could be malware run in a special "unpredictable" environment, where the OS intentionally introduces some unpredictability to the way they operate.

"Even though it seems crazy to impact functionality, it can be very effective at countering attacks if it only impacts software that could be malicious," Oliveira said. "The malicious process thinks it's in control, but it's not."

Programs you know and trust could be approved to run in a standard environment where they'll function normally, while detected malware are sequestered in a third environment, called deceptive. Instead of squashing them immediately, Chameleon would let the malicious processes continue to work in a façade environment while collecting information that can be used to understand and defeat them.

Oliveira's inspiration came in part from her interest in military strategy.

"I've read a lot about warfare. Sun Tzu, Julius Caesar - they were

successful because of the element of surprise. Cyberwarfare is the same," she said.

Deception has been used against cyber-attacks before, mostly in "honeypot" strategies that lure attackers in to gather information. But those deceptions typically are quickly revealed, Oliveira says, which limits their effectiveness. What sets Chameleon apart is inconsistent deception: Software that has been quarantined - or malware that bypasses standard detection systems - runs in an unfavorable environment until proven either benign or malicious.

An operating system like Chameleon would be great for a corporate environment, where the mission-critical software is known in advance, Oliveira says. That's good news not just for corporations, but also for those of us who entrust our sensitive data to them.

"Predictable computer systems make life too easy for attackers," she said.

Provided by University of Florida