Cybersecurity system evolves as it watches and learns from would-be hackers

January 16 2019, by Rebecca Jones

To “hack” a hacker, a VCU Engineering professor co-created a system that often deploys honeypots, shadow systems that appear to be legitimate parts of the grid but that actually divert, trap and quarantine malicious actors. Credit: VCU College of Engineering

For hackers, the United States energy grid is a treasure trove of

classified information with vast potential for profit and mayhem. To be effective, the power grid's protection system has to be a bit like a hacker: highly intelligent, agile and able to learn rapidly.

Milos Manic, Ph.D., professor of computer science in the Virginia Commonwealth University College of Engineering and director of VCU's Cybersecurity Center, along with colleagues at the Idaho National Laboratory, has developed a protection system that improves its own effectiveness as it watches and learns from those trying to break into the grid. Their Autonomic Intelligent Cyber Sensor was recognized recently at the 2018 R&D 100 Awards, an international competition that annually recognizes the 100 most promising innovations in science and technology.

'An underground war of many years'

Manic calls ongoing attempts to infiltrate the power grid—and efforts to thwart them—"an underground war of many years." These criminals aim to enter critical infrastructures, such as energy systems, to disrupt or compromise codes, screens' login information and other assets for future attacks. The result would be an infrastructure shut down in multiple locations, a so-called "Black Sky Event" that would erase bank accounts, disable cellphones and devastate the economy. In that scenario, engineers would have less than 72 hours to restore the grid before batteries, food supplies, medicine and water run out.

With high stakes and increasingly sophisticated attackers, artificial intelligence and machine learning are key to respond to the challenges of protecting the grid's interconnected systems, Manic said.

"Hackers are much smarter than in the past. They don't necessarily look at one particular component of the system," Manic said. "Often, they can fool the system by taking control of the behavior of two different

components to mask their attack on a third."

A nervous system for the power grid

Using artificial intelligence algorithms, the Autonomic Intelligent Cyber Sensor can look holistically at an array of interconnected systems, including the electrical grid, and adapt continually as attacks are attempted. It is inspired by the body's autonomic nervous system, the largely unconscious functions that govern breathing, circulation and fight-or-flight responses. Once installed, the sensor acts as a similar "nervous system" for a power grid, silently monitoring all of its components for unusual activity—and learning to spot threats that were unknown when it was first installed.

The sensor often deploys honeypots—shadow systems that appear to be legitimate parts of the grid but that actually divert, trap and quarantine malicious actors. These honeypots allow asset owners to gather information that can help identify both a threat and a potentially compromised system.

"Honeypots can make a hacker think he has broken into a real system," Manic said. "But if the hacker sees that the 'system' is not adequately responding, he knows it's a honeypot." For this reason, the system's honeypots are also intelligently updating themselves.

Manic developed AICS with his Idaho National Laboratory colleagues Todd Vollmer, Ph.D., and Craig Rieger, Ph.D. The AICS team formed eight years ago, and Manic continued to work on the project when he came to VCU in 2014. He holds a joint appointment with Idaho National Laboratory.

Provided by Virginia Commonwealth University