Student devises novel way to detect hackers

April 8 2014, by Todd R. Mcadam

Patricia Moat gets a thrill from protecting people. As a youngster, she trained in martial arts. Later, she ran into burning buildings as a volunteer firefighter. Now she's finding new ways to protect American computer networks.

"This is like catching an intruder coming into your house," Moat says. "And it excites me to do something most people have never done."

Moat, a doctoral student in electrical and computer engineering, is part of a Binghamton University team working to create a real-time monitor that can spot intrusions into computer networks.

The project, funded by the Air Force Office of Scientific Research, connects several threads in Moat's life. She's an electrician's daughter who was as interested in coding as wiring. Her brother is a career soldier. And she survived a house fire when she was a child.

Her work is critical to every nation and most corporations. Already, South Korea has found North Korea hacking its networks. Saudi Arabia and Israel have weathered cyber attacks from Iran.

Now imagine an attack that causes planes to land short of the runway, says Victor Skormin, a distinguished service professor and Moat's advisor. Imagine nuclear power plants shutting down or overheating. How about power grids misdirecting electricity? It's not just some amateur hacker against a national or corporate network; many attacks are sponsored by other nations or large criminal organizations. And they can

target computer-controlled machinery.

"Actually, it's a war taking place in cyberspace, and it requires many different weapons and defenses," Skormin says. "There are many existing attacks that our application works against very successfully."

So what are Moat and her teammates doing? Instead of reviewing all programs run by a network to find the signature of one of millions of known malware programs—some of which mutate to avoid detection—they have developed a technology to assess behavior of individual computers. This is done by monitoring system calls, the internal signals that accompany every computer operation and can reveal every function performed by the computer.

First, they create a profile of the network's normal operation. When a network is attacked, a review of system calls can reveal functionality that does not match this "normalcy profile." This approach can address the most advanced attacks, some of which are skillfully designed to corrupt just one strategically chosen computer system.

Think of it this way: Instead of looking for an intruder in your home by checking every room to see if anything has been taken or left behind, the Binghamton algorithm checks to see if anyone opened a door or window.

Provided by Binghamton University