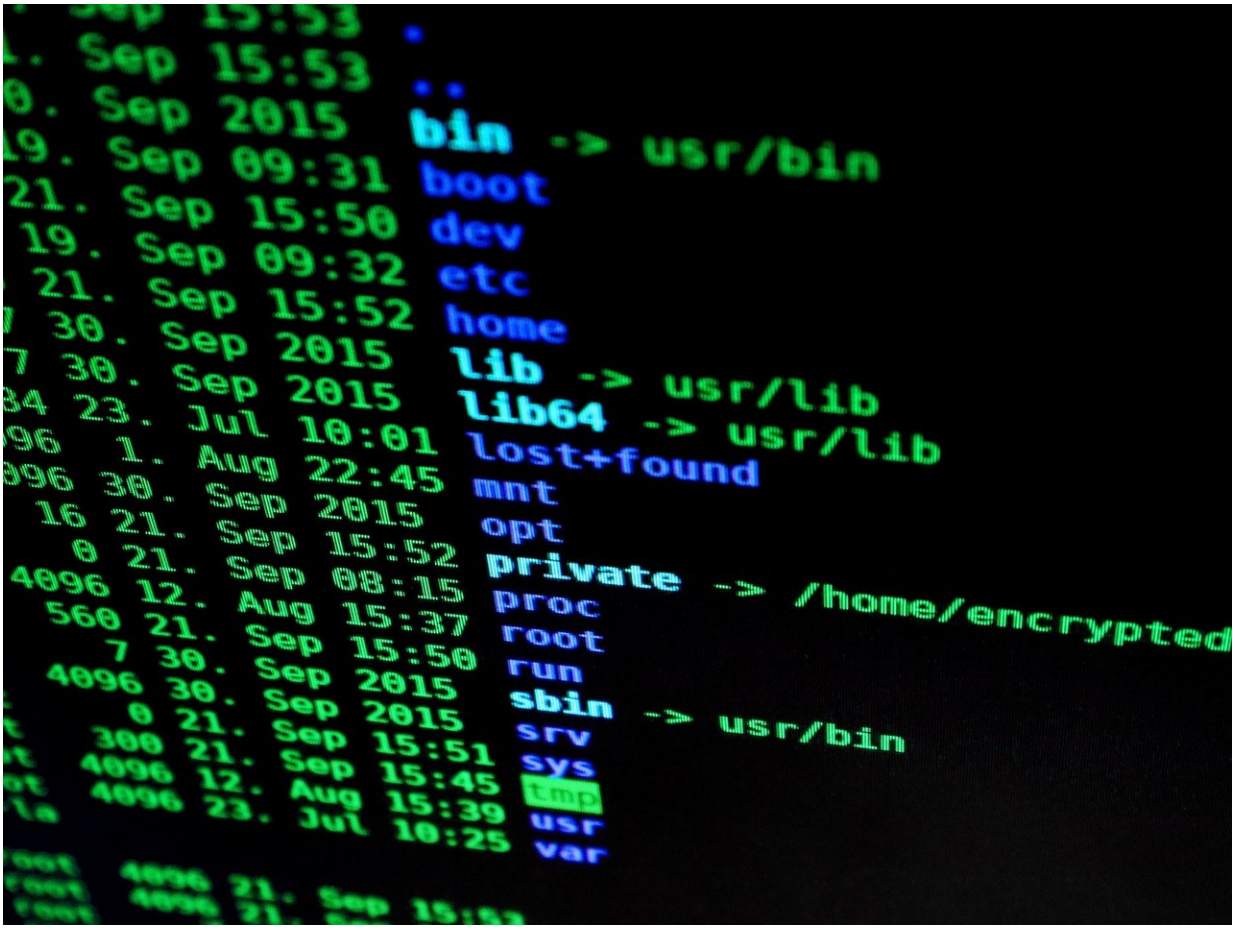
Cyber of the fittest: Researchers develop first cyber agility framework to measure attacks

June 10 2019, by Milady Nazir



Credit: CC0 Public Domain

For more than a year, GozNym, a gang of five Russian cyber criminals,

stole login credentials and emptied bank accounts from unaware Americans. To detect and quickly respond to escalating cyber-attacks like these, researchers at The University of Texas at San Antonio (UTSA) have developed the first framework to score the agility of cyber attackers and defenders. The cyber agility project was funded by the Army Research Office.

"Cyber agility isn't just about patching a security hole, it's about understanding what happens over time. Sometimes when you protect one vulnerability, you expose yourself to 10 others," said computer science alumnus Jose Mireles '17, who now works for the U.S. Department of Defense and co-developed this first known framework as part of his UTSA master's thesis. "In car crashes, we understand how to test for safety using the rules of physics. It is much harder to quantify cybersecurity because scientists have yet to figure out what are the rules of cybersecurity. Having formal metrics and measurement to understand the attacks that occur will benefit a wide range of cyber professionals."

To develop a quantifiable framework, Mireles collaborated with fellow UTSA student Eric Ficke, researchers at Virginia Tech, U.S. Air Force Research Laboratory, and the U.S. Army Combat Capabilities Development Command Army Research Laboratory (CCDC ARL). The project was conducted under the supervision of UTSA Professor Shouhuai Xu, who serves as the director of the UTSA Laboratory for Cybersecurity Dynamics.

Together, they used a honeypot—a computer system that lures real cyber-attacks—to attract and analyze malicious traffic according to time and effectiveness. As both the attackers and the defenders created new techniques, the researchers were able to better understand how a series of engagements transformed into an adaptive, responsive and agile pattern or what they called an evolution generation.

The framework proposed by the researchers will help government and industry organizations visualize how well they out-maneuver attacks. This groundbreaking work will be published in an upcoming issue of IEEE Transactions on Information Forensics and Security, a top cybersecurity journal.

"The cyber agility framework is the first of its kind and allows cyber defenders to test out numerous and varied responses to an attack," said Xu. "This is an outstanding piece of work as it will shape the investigation and practice of cyber agility for the many years to come."

"The DoD and US Army recognize that the Cyber domain is as important a battlefront as ground, air and sea," said Purush Iyer, Ph.D. division chief, network sciences at Army Research Office, an element of CCDC ARL. "Being able to predict what the adversaries will likely do provides opportunities to protect and to launch countermeasures."

Mireles added, "A picture or graph in this case is really worth more than 1,000 words. Using our framework, security professionals will recognize if they're getting beaten or doing a good job against an attacker."

Provided by University of Texas at San Antonio