Lab licenses tool to improve government computer network security

January 5 2016

Credit: George Kitrinos/LLNL

Government agencies, along with state and local governments, could receive a helping hand from a computer network security tool developed by computer scientists and engineers at DOE's Lawrence Livermore National Laboratory.

The LLNL software-based technology, known as the Network Mapping System (NeMS), has been licensed to Cambridge Global Advisors, a Washington, D.C.-area strategic advisory firm.

"We developed this capability to discover and characterize computer networks," said Celeste Matarazzo, a principal investigator for cybersecurity in the Lab's Global Security Principal Directorate. "It is important to know what you have on your networks, so that you can decide what best practices to apply."

Rich Rankin, the director of LLNL's Industrial Partnerships Office, called the commercialization of NeMS "a significant step forward in protecting the nation's network environment."

In effect, NeMS provides network managers with a comprehensive view of their computer network environments. It has been used at different times to support the computer network security operations at several federal agencies.

"What NeMS helps you do is to discover the things you didn't know about your computer network," Matarazzo said, adding that network discovery is one of three key functions provided by NeMS.

If a rogue computer has access to a computer network, it won't be using a company's virus protection system, she said. The goal is to uncover any unauthorized devices to ensure a company is not at risk.

A second service provided by NeMS is the capability to identify which computers are communicating, the structure of the network, the protocols used in communication and other attributes of the organization's computer network.

Finally, NeMS permits security and information technology professionals to conduct their own customized analysis of computer network environments of interest, Matarazzo said.

Nearly all of the commercial network monitoring and visualization tools currently available work in either passive mode, which "watches" activity between network targets, or active mode, which scans and probes a network. NeMS combines the two modes—collecting data by watching and probing the network—to more fully characterize the operating environment.

NeMS' scans and analysis can reveal valuable information such as misconfigurations and other system errors that might make a network vulnerable to attack.

NeMS can characterize a network from multiple vantage points, and merges the results into a single data store for analysis. The software's monitoring and characterization tools can generate a new map, corroborate or update existing maps or fuse the data collected with additional information on an organization's network.

The commercial licensing of NeMS was aided by the Department of Homeland Security's "Transition to Practice Program," which Matarazzo called "a very valuable experience."

"We met entrepreneurs and have been able to present our capabilities to a wide variety of audiences—Silicon Valley, the energy sector in Houston, the financial sector in New York and others.

"We've been exposed to the entrepreneurial process, the venture capital community and have had some very engaging discussions about where NeMS could go," Matarazzo said.

She described the NeMS team as computer scientists and engineers who are collaborative and productive, with a passionate mission to improve computer security. Other team leaders included computer engineer Domingo Colon and NeMS project manager and computational physicist Evi Dube.

The NeMS software has been developed over the past 15 years, with a major rewrite of the code in 2011 and a push in 2013 into advanced research directions through internal Laboratory Directed Research and Development funding.

Provided by Lawrence Livermore National Laboratory