Mapping Networks for Cyberdefense

NEWS reports routinely warn computer users about Internet bugs that threaten the security of important personal information stored online. Large corporations and government agencies are even more vulnerable to bugs and hacking schemes, which may expose critical data that can be used for nefarious purposes. Even with the known potential for damage, few organizations have a complete picture of their vast networks.

Lawrence Livermore has developed a software-based tool called Network Mapping Systems (NeMS) to provide network owners with a comprehensive view of their computer network environments. NeMS builds these visual maps based on observed behavior on the network. It also offers an iterative analysis platform that cybersecurity and information technology personnel can use to explore the maps generated.

"NeMS is a tool for discovering what is actually on a network," says computer scientist Celeste Matarazzo, who worked with colleagues from the

Laboratory's Computation and Engineering directorates to develop the application. A NeMS scan can reveal valuable information such as misconfigurations and other system errors that might make a network vulnerable to attack.

Watching and Probing the Operating Environment

Understanding the components and structure of a computer network and how those resources are used is the first step in many cyberdefense and mission-assurance operations. Mapping software provides a detailed view of a network's topology, including the routers, switches, and end hosts connected to the system and the services running on those devices.

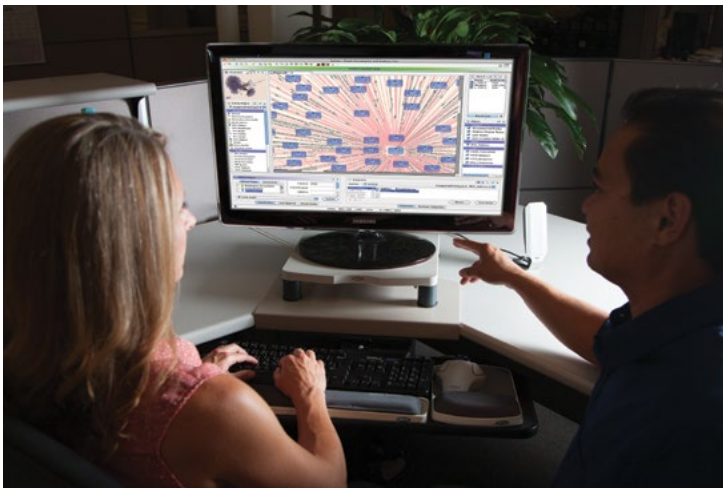
The commercial mapping tools currently available work in either passive mode, which "watches" activity between network targets, or active mode, which scans and probes a network. NeMS combines the two modes—collecting data by watching and probing the network—to more fully characterize the operating environment. NeMS runs on dedicated computer hardware so that scanning does not interfere with network performance and to provide a platform for follow-on analysis. The application can also be implemented as a virtual machine with all the tools needed for mapping, allowing it to operate behind a firewall, on a disconnected system, or on a geographically or logically separated network.

NeMS can characterize a network from multiple vantage points, and merges the results into a single data store for analysis. The software's visualization tools can generate a new map, corroborate or update existing maps, or fuse the data collected with additional information on an organization's network. Having a complete map of the observed operating environment provides what Matarazzo calls "full situational awareness" of the assets, attributes, roles, and logical relationships within a network.

"Computer networks are complex and organic, changing all the time," says Matarazzo. "A NeMS map provides a snapshot of a network's current structure and activity. Repeated mapping offers a picture of how a network is being used and discovers changes that may reveal weak spots or vulnerabilities."

According to Matarazzo, system administrators determine which parts of a network should be characterized. "NeMS does not break through firewalls or scan prohibited areas," she says. "It operates within the parameters set by each client." The mapping routines in NeMS work effectively without extensive preparation or prior knowledge of a network and do not compromise the security posture of the mapped environment. In contrast, current network-mapping tools can be slow and intrusive, and many require special exceptions to network security.

To validate the accuracy of the NeMS mapping techniques, the Livermore team tested the system in both controlled and operational environments. Controlled testing evaluates a network that is offline or otherwise isolated from live (production) operations. In a test with ground-truth information (data similar to that on an active system), NeMS not only identified 100 percent of the network's hosts but also discovered an unknown connection to an external network. The test engineers confirmed that this unexpected connection was in fact valid.



The Livermore-designed Network Mapping Systems (NeMS) collects data by watching and probing a network. It runs on dedicated computer hardware to maintain performance on the network being scanned and to provide a platform for follow-on analysis.

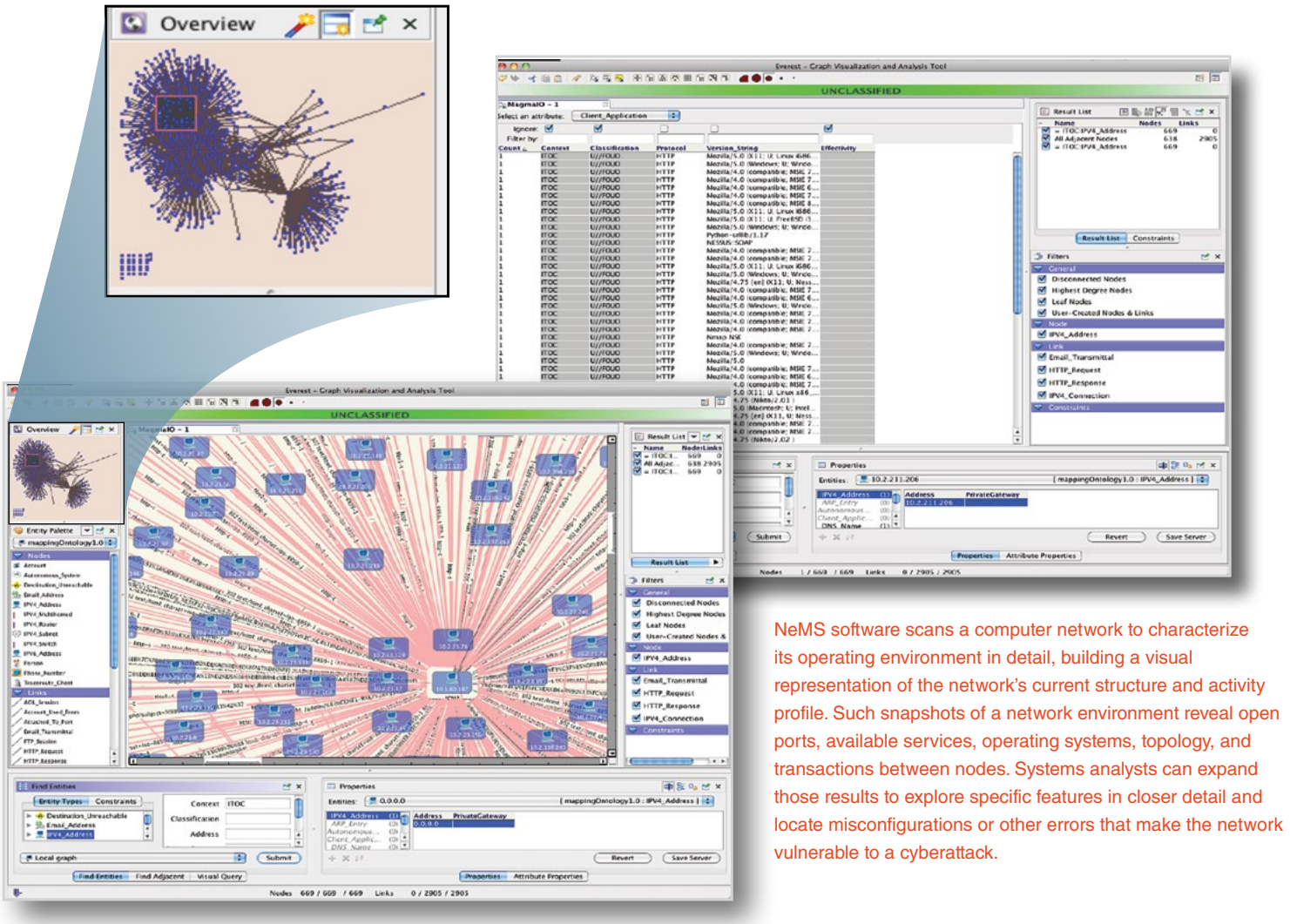
A Plan for Commercialization

The NeMS development team has submitted a patent application on various aspects of the software tool and is working with the Laboratory's Industrial Partnerships Office to find a licensee to commercialize the technology for broader adoption by state and local governments and by private industry. Matarazzo notes that a licensee would have customer service resources not available at a national laboratory and could design a more user-friendly interface for the software.

In product commercialization, developing a new technology is often viewed as the easy part of the process. The more difficult stage is making the technology simple to use and transferring it to a licensee who can effectively market and support the product. This stage has been termed the valley of death because many technologies languish here, often forever.

In 2011, the Department of Homeland Security's Cyber Security Division established the Transition to Practice (TTP) Program to help bridge the valley of death. The program was created in response to the White House's Federal Cybersecurity Research and Development Strategic Plan and the Comprehensive National Cybersecurity Initiative. Its goal is to connect developers from national laboratories with potential licensees and accelerate the transfer of cybersecurity technologies developed with federal funding to a broad audience.

NeMS was a sponsored technology during TTP's first year, and Matarazzo attended the program's May 29, 2014, Technology Demonstration Day for the Energy Sector in Houston, Texas. The



NeMS software scans a computer network to characterize its operating environment in detail, building a visual representation of the network's current structure and activity profile. Such snapshots of a network environment reveal open ports, available services, operating systems, topology, and transactions between nodes. Systems analysts can expand those results to explore specific features in closer detail and locate misconfigurations or other errors that make the network vulnerable to a cyberattack.

event's presentations and demonstrations featured nine technologies from federally funded research and development centers under the Departments of Energy and Defense, each one addressing a unique cybersecurity issue. Attendees—cybersecurity professionals from the energy sector—learned about opportunities for piloting the new technologies and discussed their organizations' areas of interest for future cybersecurity research.

Staying Ahead of Security Threats

Computing and network technology are changing at a rapid pace, often introducing unidentified vulnerabilities. To stay ahead of cybersecurity threats, Matarazzo is leading a Laboratory Directed Research and Development project to take network mapping to the next step. This work involves a larger Livermore team and partners at four universities: Carnegie Mellon, Rutgers, Purdue, and University of California at Davis. The collaboration's new tool, called Continuous Network Cartography, will provide a better understanding of complex or obfuscated computer networks by repeatedly mapping components, services, applications, and their dependencies, showing how they change over time.

Many of the most critical operations in the Departments of Defense, Energy, and Homeland Security depend on complex networks, as do electric smart grids and other parts of the national infrastructure. Decision makers and network operators need to understand an entire network as it evolves, so they can manage assets in a way that prevents intrusions or system failures while allowing defined tasks and missions to be accomplished.

—Katie Walter

Key Words: Continuous Network Cartography, cybersecurity, Department of Homeland Security Transition to Practice (TTP) Program, Network Mapping Systems (NeMS).

For further information contact Celeste Matarazzo (925) 423-9838 (matarazzo1@llnl.gov).