Tri-City Herald – PNNL Research is Enhancing Cybersecurity (5/16/16):
http://www.tri-cityherald.com/news/local/pacific-northwest-national-lab/article77790282.html

May 15, 2016 3:14 PM

PNNL research is enhancing cybersecurity

Highlights

- One initiative focuses on enabling computer network to know when it's under attack and take actions
- Another effort uses 'ants' that wander from device to device in a network to find, intervene with anomaly
- Tool also developed to simultaneously assess cybersecurity, physical security

By Steven Ashby, Director, Pacific Northwest National Laboratory

Cybersecurity is increasingly top-of-mind and in the news. Individuals worry about identity theft and the compromise of financial and medical records. Companies struggle to stay one step ahead of criminal hackers looking for customer data and corporate secrets. And the federal government battles myriad threats aimed at our national security and critical infrastructure.

At the Department of Energy's Pacific Northwest National Laboratory in Richland, we are working hard to address these threats. We conduct basic research in computer science to understand the inherent vulnerability of computer systems and networks, and we develop tools that help protect them.

Our sophisticated software tools can monitor a network in real time, watching for anomalous behavior and take defensive actions when an intruder is detected. We deploy these tools to protect our own network and those at other DOE sites, as well as to protect critical infrastructure like the power grid.

One of our research initiatives focuses on developing self-healing, resilient cyber environments. The goal here is to enable a computer network to know when it is under attack and to take actions to isolate the attacker and minimize the damage. To do this, we bring together researchers with expertise in computer science, mathematics, systems engineering and even social science. Beyond understanding the technology, we also need to understand how computer users behave — for example, what makes them susceptible to phishing attempts.

Another research effort, inspired by nature, led to a cyber defense tool that mimics how seemingly independent ants can quickly communicate with one another and coordinate their efforts to swarm and protect their colony. The tool's small ant-like programs wander from device to device on a network. If one detects something unusual, it leaves a signal that attracts more ants to check out the anomaly. The resulting "swarm" is a signal that further investigation and possible intervention is warranted. This approach was recognized among Scientific American's "10 world-changing ideas" in 2010.

Cyberattacks are happening more frequently, but they also are becoming increasingly sophisticated. In particular, the line between cybersecurity and physical security is blurring. To uncover risks that might go unnoticed if the cyber and physical domains were examined independently, we have developed a first-of-its-kind tool that simultaneously assesses both kinds of risks. For example, it evaluates cyber-enabled physical vulnerabilities, like hacking into a security system to disable alarms, as well as physical-enabled cyber vulnerabilities, like breaking into a data storage center to steal sensitive data.

The line between cybersecurity and physical security is blurring.

This tool was licensed to a small business, RhinoCorps, through a Department of Homeland Security technology transfer program earlier this year.

PNNL is applying its expertise in cybersecurity to protect the electrical grid, including a suite of technologies and tools that help utilities protect their portions of the grid. In one DOE program, called CRISP (Cyber Risk Information Sharing Program), utilities voluntarily share high-level network traffic information with PNNL so that our experts can analyze it for potential threats to the individual utility or the broader interconnected system.

Cooperative efforts like this are enabled by our ongoing engagement with the utility industry. For example, we co-hosted the third annual Washington State Cybersecurity Summit with the Snohomish County Public Utility District in February to bring together industry leaders and policy makers to discuss a comprehensive approach to grid security. Participants at forums like these share experiences and develop a common approach to address the challenges we all face.

PNNL also applies its expertise and tools to protect an asset a bit closer to home: the laboratory itself.

Each day, our cyber firewall systems block 24 million suspect Internet communications, more than 25,000 of which are known to be cyberattacks directed at PNNL. This requires us to analyze huge amounts of data in real time — which we can do because of our “big data” expertise and supercomputing power. On the rare occasion that a hacker is successful, we can typically analyze the attack, isolate it and recover quickly. We also help DOE manage its cyber risk by analyzing about a billion events each day collected at 100 locations across the DOE system.

24 million

Number of suspect Internet communications, more than 25,000 of which are known to be cyberattacks directed at PNNL, that the Richland lab firewall systems block

Our secret weapon in the fight for cybersecurity is our talented staff. We have an amazing group of cyber defenders at the lab — but we need more. Given the huge need across the country for this kind of skill, Battelle, which manages PNNL, funded a cybersecurity program at Columbia Basin College that is helping prepare the next generation of experts who will fight cyberattacks and thwart data breaches.

I have highlighted just a few examples of how PNNL is helping to promote greater cybersecurity through world-class research and innovative tools. We will continue to do our part. And you can help too: make sure that you have anti-virus software installed on your personal and business computers, use passwords and back up your valuable data.

Steven Ashby, director of Pacific Northwest National Laboratory, writes this column monthly.