

New brain-inspired cybersecurity system detects 'bad apples' 100 times faster

March 21 2017



Sandia National Laboratories' Roger Suppona, left, and John Naegle, center, and Lewis Rhodes Labs CEO David Follett examine their Neuromorphic Cyber Microscope. This small processor can replace racks of conventional cybersecurity systems. Credit: Randy Montoya

Cybersecurity is critical—for national security, corporations and private

individuals.

Sophisticated cybersecurity systems excel at finding "bad apples" in computer networks, but they lack the computing power to identify the threats directly.

Instead, they look for general indicators of an attack; call them "apples." Or the [system](#) flags very specific patterns, such as "bad Granny Smith apples" or "bad Red Delicious apples."

These limits make it easy for new species of "bad apples" to evade modern cybersecurity systems. And security analysts must sort the real dangers from false alarms, such as the nonsense phrase "forbad applesauce."

The Neuromorphic Cyber Microscope, designed by Lewis Rhodes Labs in partnership with Sandia National Laboratories, directly addresses this limitation. Due to its brain-inspired design, it can look for the complex patterns that indicate specific "bad apples," all while using less electricity than a standard 60-watt light bulb.

From cerebral palsy to a cybersecurity system

The processor in the Neuromorphic Cyber Microscope is based on the neuroscience research of Dr. Pamela Follett, a co-founder of Lewis Rhodes Labs. Follett is a pediatric neurologist and neuroscientist who studies developmental diseases, such as [cerebral palsy](#) in children. Her husband, David Follett, co-founder and CEO of Lewis Rhodes Labs, used her work as the basis for a computational model of how the brain processes information.

Comparing brains with cerebral palsy to healthy brains was key to the deeper insights. The Folletts built brain-inspired computer

hardware—hardware they knew could solve some real-world problems. Enter Sandia, with a long history of solving real-world challenges.

A team led by computer systems expert John Naegle sought problems where the neuromorphic processor would excel. The team looked at robotics and [pattern](#) recognition before settling on cybersecurity.

"We quickly realized that we could use this architecture to greatly accelerate our ability to look for patterns and even look for complex versions of these patterns," said Naegle.

Brain inspiration leads to faster, more efficient threat detection

Both the Neuromorphic Cyber Microscope and the human brain continually scan for threats. A hose or stick can cause you to jump, even if you're not searching for a snake. Similarly, the Neuromorphic Cyber Microscope compares streaming data to suspicious patterns in a time-dependent manner. In contrast, conventional cyberdetection systems sequentially match small chunks of data against a library of "bad apple" patterns, which is less efficient, said Naegle.

Sandia tested the Neuromorphic Cyber Microscope on its cybertraffic in a demonstration environment. As the "bad [apple](#)" patterns got more complex, the state-of-the-art conventional system slowed exponentially, but the Neuromorphic Cyber Microscope kept performing efficiently, said Roger Suppona, a cybersecurity expert at Sandia.

In fact, it's more than 100 times faster and 1,000 times more energy-efficient than racks of conventional cybersecurity systems. "This completely changes the way that we look for suspicious activity without running the risk of overwhelming our analysts with too much

information," said Suppona.

The Neuromorphic Cyber Microscope, an R&D100 Awards finalist this year, is in the early stages of deployment.

Sandia and Lewis Rhodes Labs are exploring what else they can do with the general neuromorphic architecture. They've explored a type of machine learning that is used for audio and image processing and sorting numbers efficiently. Naegle said they're still in early stages, looking at fundamental algorithms. This basic research is supported by Sandia's Laboratory Directed Research and Development program. Naegle said, "Eventually, we'd like to have completely new algorithms that really take advantage of the way the brain actually does its operations."

David Follett has worked with Sandia off and on for more than 20 years. His earlier company jointly won an R&D100 award in 1996 for the ATM OC-12c Protocol Engine, a fast interconnect for computer-network communications.

"Sandia has a very unique culture and extraordinarily talented people," he said. "The technical breadth of the lab and domains where they have world-class expertise is very impressive. It's an ideal environment for incubating novel, disruptive technologies like the Neuromorphic Cyber Microscope."

Provided by Sandia National Laboratories

Citation: New brain-inspired cybersecurity system detects 'bad apples' 100 times faster (2017, March 21) retrieved 19 April 2024 from <https://phys.org/news/2017-03-brain-inspired-cybersecurity-bad-apples-faster.html>

This document is subject to copyright. Apart from any fair dealing for the purpose of private

study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.