

# Researchers enable real-time forensic analysis with new cybersecurity tool

August 29 2018, by Scott Jones

---



ORNL cybersecurity researchers Jared Smith (left) and Elliot Greenlee (right) participate in a demonstration day event to showcase how Akatosh, a new security analysis tool, quickly sorts through data to identify potential threats. Credit: Oak Ridge National Laboratory

As technology continues to evolve, cybersecurity threats do as well. To

better safeguard digital information, a team of researchers at the US Department of Energy's (DOE's) Oak Ridge National Laboratory (ORNL) has developed Akatosh, a security analysis tool that works in conjunction with standard software to detect significant irregularities in computer networks.

"Akatosh is a system that provides deeper context to existing IT infrastructure designed to solve [security](#) problems," said Jared Smith, a cybersecurity researcher in ORNL's Computing and Computational Sciences Directorate (CCSD) who developed the new technology. "It gives you a historical look of what's changing on a computer over time."

This new resource coordinates with [intrusion detection systems](#) (IDSs), which monitor computer networks for private companies, government facilities, and academic institutions and set off alerts in response to abnormal activity. IDSs tend to trigger false alerts, forcing cybersecurity analysts and IT professionals to manually search the network for changes.

"Any organization with a lot of people using computers will get thousands of alerts a day, and someone has to sift through them," Smith said. "The typical tools available provide a bunch of data that analysts have to look at to decide whether or not the system has actually been breached."

Akatosh saves precious time and resources previously consumed by this tedious process by periodically taking snapshots of host systems on the network during everyday operations and establishing a baseline, then taking another snapshot each time an IDS alert occurs. By comparing these snapshots, Akatosh can immediately show changes that transpired leading up to and during a cyber event. Automating the process of sorting through IDS alerts reduces the time and cost required to identify the source of a security incident and neutralize the threat.

"At a technical level, we can see whether passwords are being extracted, whether files are being copied, and we know how these things are potentially threatening because they weren't happening before we got an alert," Smith said. "That's where we're able to provide context."

The system summarizes relevant changes and sends a report to the network administrator to quickly determine whether the changes indicate the presence of a legitimate security threat. The ability to accurately determine the validity of IDS alerts in real time means analysts can begin mitigating the negative effects of malware attacks, phishing emails, and other cybersecurity problems as soon as they appear.

"Akatosh solves such a widespread efficiency problem by dealing with incidents on a network much faster, which allows us to allocate our time better. It provides a more targeted way to weed out unimportant data and reveal areas of concern," said Smith, who has been working on Akatosh since he first arrived at ORNL as an intern in 2015.

After becoming a staff member in the Cyber and Information Security Research Group (CISR) of CCSD's Computational Sciences and Engineering Division in 2017, he has served as principal investigator for the project in collaboration with a team of software engineers and interns. Their work on Akatosh supports CISR's mission to defend against cyber attacks and uphold the security of information and infrastructure nationwide.

To demonstrate Akatosh's dynamic capabilities, the team recently traveled to San Francisco for RSA, the largest security conference in the country. They also attended US Department of Homeland Security (DHS) summits in New York and Washington, DC.

"It's been a lot of fun to travel and demo Akatosh for people," Smith said. "We actually use real malware and show how, once it spreads

across the machine, we can see how it changes and pinpoint the problem."

Provided by Oak Ridge National Laboratory

Citation: Researchers enable real-time forensic analysis with new cybersecurity tool (2018, August 29) retrieved 9 April 2024 from <https://phys.org/news/2018-08-enable-real-time-forensic-analysis-cybersecurity.html>

<p>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.</p>
--