OAK RIDGE NATIONAL LABORATORY

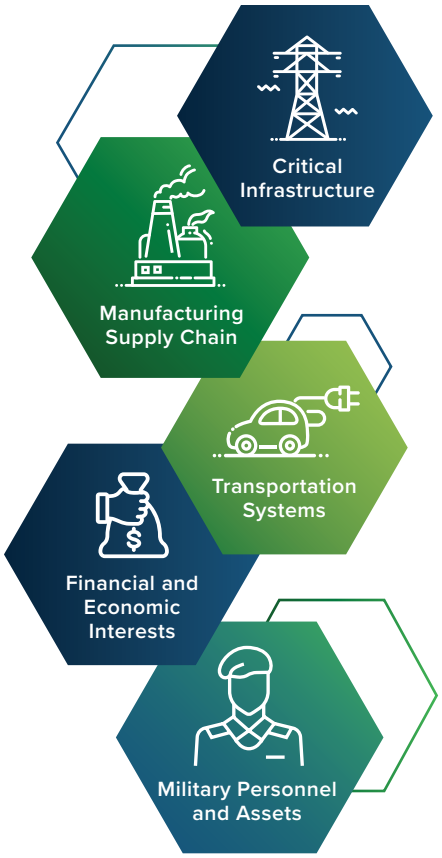
Systems Vulnerability

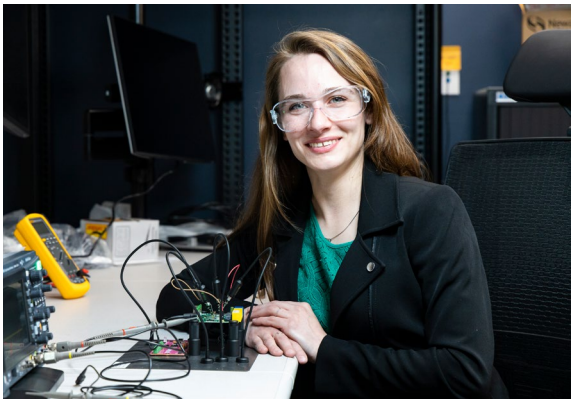
As cell phones, cars, industrial machinery, the electric grid, and even home appliances become constantly more connected into complex networks, they both offer new capabilities and present a new kind of target to antagonists. ORNL experts are working to protect U.S. systems of defense, energy, and transportation by identifying their vulnerabilities, recognizing how hostile actors might exploit them, and finding ways to eliminate the risks.

ORNL expertise in system vulnerabilities, reverse engineering, program analysis, programming languages and computational theory is crucial to test software and firmware, the embedded code that runs in devices ranging from cars to the power grid. Tools and practices developed by ORNL researchers are key to reducing the nation's risk in the face of cyber-spying and cyberattack.

CAPABILITIES

- Perform static analysis of source code and binary images to find mistakes made by humans or automatic code generators that weaken a program, potentially allowing it to be used in a different way than intended
- Wield advanced dynamic analysis tools such as machine learning and symbolic execution (solving conditional statements within computer programs mathematically) to identify vulnerabilities, breaches, or attacks
- Recognize and study new adversarial tools, such as malware, as they emerge, identifying the signs and patterns that reveal their presence
- Utilize deep expertise in programming languages, architecture, and machine types to reverse engineer programs, malware, and other adversarial cyber tools, expanding understanding of their functions and origins
- Emulate different types of systems to observe how they function and learn to recognize abnormalities in their behavior
- Identify techniques to eliminate vulnerabilities in critical systems
- Partner with power companies and manufacturers to improve cybersecurity and build trust in key infrastructure components and their supply chains





UNIQUE PROJECTS & FACILITIES

- **The Embedded Systems Lab** facilitates the analysis of hardware and software for vulnerabilities as well as signs of tampering and malware. The lab offers a variety of tools, from nanoprobes to X-ray machines, for accessing and examining signals, microchips, and other components of computers, Internet-of-Things devices, SCADA systems, and industrial control systems.

- **CyTRICS** is a DOE-sponsored partnership among researchers and industry stakeholders to perform cybersecurity testing on high-priority operating components for the power grid. Software and hardware unit components are catalogued, vulnerabilities shared with stakeholders, and design and manufacturing improved.

- **Glass Onion** utilizes emulation to analyze firmware and software behavior as it runs, identifying and mitigating vulnerabilities before they are deployed in live systems such as the power grid and water supply.

CONTACT | Shaun Gleason | Division Director | gleasonss@ornl.gov | 865-341-1849

Oak Ridge National Laboratory is managed by UT-Battelle LLC for the US Department of Energy

OAK RIDGE National Laboratory | U.S. DEPARTMENT OF ENERGY | Office of Science

NATIONAL SECURITY SCIENCES