OAK RIDGE NATIONAL LABORATORY

Cybersecurity Science

Intrusions and attacks to computer networks are an increasing threat to U.S. defense, the economy, and critical infrastructure. The resulting theft of state secrets, financial information and intellectual property endangers human lives and causes billions of dollars in damages. New types of cyberattacks are being designed every day, so network operators need tools to help identify suspicious behavior that bypasses automated security systems.

ORNL's innovative research and development capabilities advance cutting-edge, data-driven defensive cybersecurity architectures, technologies, and evaluation methods.

RESEARCH FOCUS AREAS

Uncovering Cyber Weaknesses

- Developing high-fidelity emulators to mimic user interactions with the computer system that trigger cyber weaknesses
- Designing algorithms that can sort problems, alerts, and worthwhile cybersecurity events from a broad data processing platform and then improve the security of the platform
- Utilizing machine learning to detect and analyze malicious polyglot files capable of opening in different formats, potentially hiding their range of functions from the user

Evaluating Cyber Defenses

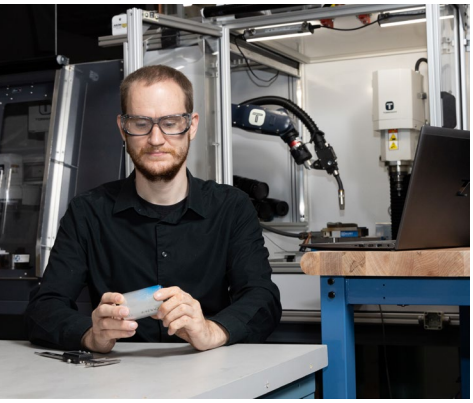
- Evaluating cyber defenses against an array of threats, from intrusion to novel malware
- Testing artificial intelligence-based cyber defenses to identify and thwart ways they can be tricked, either during the machine learning process or through manipulated data

Increasing Vehicle Cybersecurity

- Developing an algorithmic pipeline to decode the internal network signals among vehicle subsystems, enabling transparency of useful information like real-time emissions performance
- Protecting vehicle security, including sensors and internal communications networks embedded in vehicles, from outside tampering or control

Enhancing Network Security

- Developing machine learning for resetting the cyber "keys" to networked edge devices (such as Internet-connected home thermostats, network routers, and smartphones), so nodes that leave the network can't later be used to "unlock" it for unintended users



UNIQUE PROJECTS & FACILITIES

- **The Cyber Operations Research Range** is a full-scale virtual test bed for large-scale cybersecurity experiments, which can be used to evaluate and emulate malware defenses, user behaviors, and other cyber behaviors in a live setting.

- **The Vehicle Security Laboratory**, a component of ORNL's National Transportation Research Center, is dedicated to assessing cyber vulnerabilities while vehicles are in operation, including scanning for onboard computer signal interception, malware discovery and authentication and privacy protections.

- **The Controller Area Network Intrusion Detection System (CAN-IDS)** enhances the security of controller-area networks used for real-time communication among systems in vehicles, aircraft, and industrial facilities. ORNL is pioneering an after-market plug-in that uses self-tuning algorithms to automatically collect CAN data and train the system to detect intrusions.

- **The C-STAR** technology routes a vehicle's controller-area network through a portable sensor and security system that can be hand-carried on board a truck transporting sensitive cargo, such as nuclear or radiological materials, to detect any attempt to hack the vehicle's internal communications systems.

- **The Artificial Intelligence Applications to Autonomous Cybersecurity (AI ATAC)** program provided ORNL expertise to test submitted technology for resilience to cyberattack or efficacy at detecting cyberattack in a series of grand challenges, culminating in a hands-on user study involving analysists from around the world.

- **Cybersecurity Manufacturing Innovation Institute (CyManII)** is an initiative combining the expertise of ORNL and other national laboratories and research universities to meet the challenges of cybersecurity, smart and energy-efficient manufacturing, supply chains, factory automation, and workforce development.

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