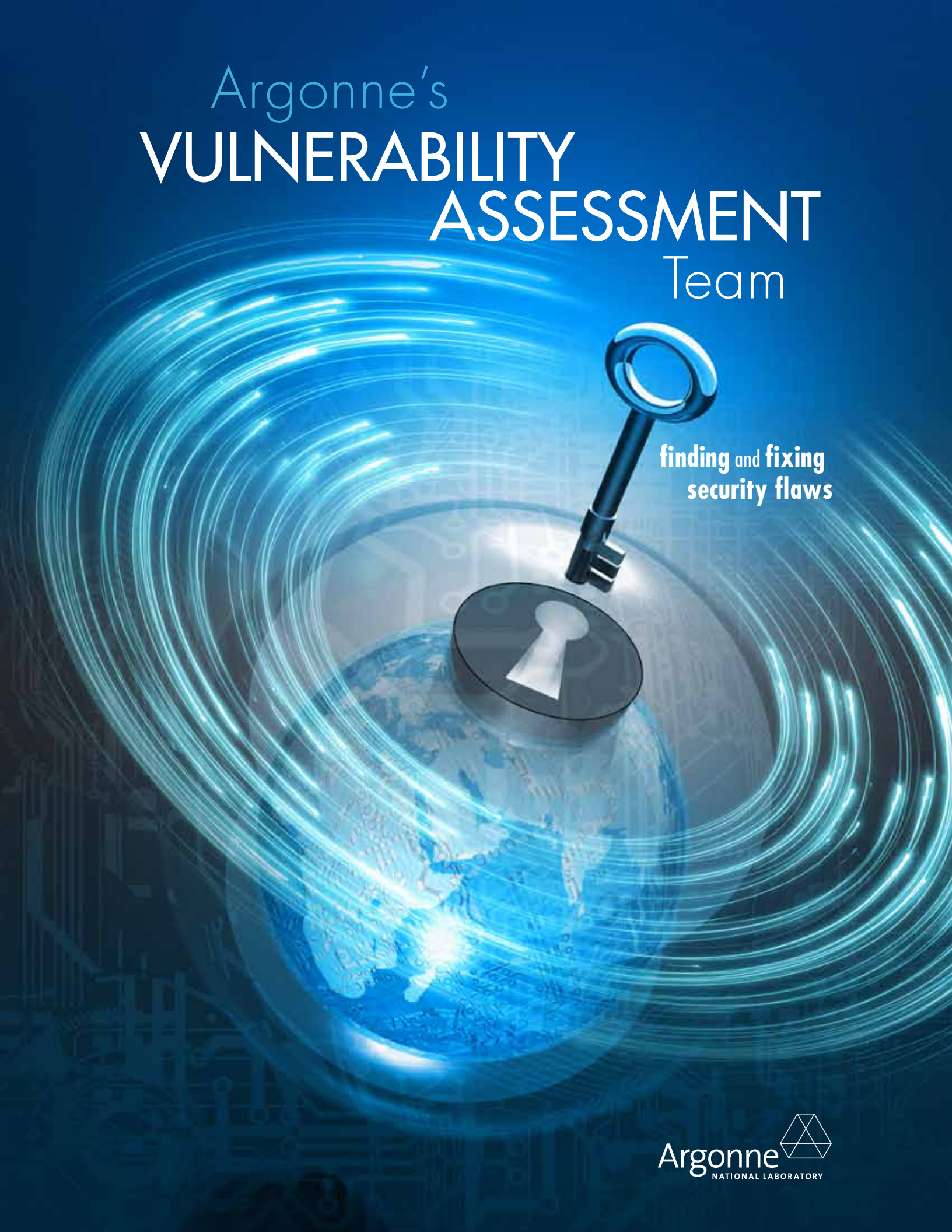
Argonne's VULNERABILITY ASSESSMENT Team



finding and fixing security flaws

Argonne NATIONAL LABORATORY

“REAL SECURITY

comes from thinking like the bad guys.”

– Roger Johnston, head of Argonne’s Vulnerability Assessment Team

Argonne’s Vulnerability Assessment Team (VAT) takes a unique approach to identifying and addressing the vulnerabilities of physical security devices, systems and programs – the team members routinely put themselves in the shoes of adversaries and in their heads as well.

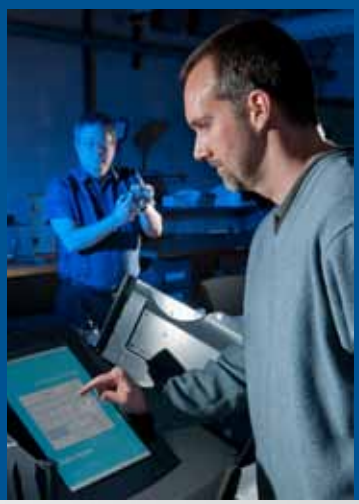
VAT researchers spend their workdays devising and demonstrating ways to defeat a wide variety of security devices, systems, and programs, ranging from electronic voting machines and global positioning systems (GPS) to nuclear safeguards programs and biometrics-based access control. This involves analyzing the security features, reverse-engineering the technology or security strategy, figuring out how to beat the security, demonstrating attacks, and then devising effective countermeasures.

The team’s “think-like-the-bad-guy” approach routinely results in the discovery of surprising, easy-to-exploit vulnerabilities that are often overlooked by security managers, designers and manufacturers, as well as other vulnerability assessors using more conventional or formalistic techniques.

The VAT has worked with more than 50 different companies, non-profits and government organizations, including the U.S. Department of Defense, National Nuclear Security Administration, Department of Homeland Security, U.S. Department of State, International Atomic Energy Agency, Euratom and intelligence agencies.

The team provides vulnerability assessments, consulting, training, and research and security solutions, including classified experimental projects. In addition to the Vulnerability Assessment Laboratory’s extensive classified lab space, team members have access to two Sensitive Compartmented Information Facilities (SCIFs).

The VAT also runs a rapid, one-stop microprocessor shop that provides quick turnaround for inexpensive microprocessor prototype circuits. These can be used to record data, control experiments, transmit data wirelessly, provide better security for instruments/cargo/packages, or demonstrate concepts.



Argonne's VAT works in the following areas:

- Cargo Security
- Election Security
- Nuclear Safeguards
- Consulting & Training
- Novel Security Strategies
- Vulnerability Assessments
- Human Factors in Security
- Security Countermeasures
- Access Control & Biometrics
- Product Tampering & Counterfeiting
- Microprocessor & Wireless Applications
- Physical/Electronic Tamper & Intrusion Detection

Sample projects:

- Rapid sampling tools for Customs & U.S. Special Forces
- GPS spoofing countermeasures
- Novel access control techniques
- Security for employee drug tests
- Security for medical devices
- Counterfeiting tags & seals
- Mitigating the insider threat
- Security culture & climate
- Physical security R&D
- Sticky bomb detection
- Reverse engineering
- Better courier bags
- Better tags & seals
- Wine authenticity

The VAT also hosts and edits the Journal of Physical Security (http://jps.anl.gov)

For more information, contact:

Roger Johnston, Ph.D., CPP

rogerj@anl.gov | 630.252.6168

www.ne.anl.gov/capabilities/vat

U.S. DEPARTMENT OF ENERGY

Argonne National Laboratory is a U.S. Department of Energy laboratory managed by UChicago Argonne, LLC.