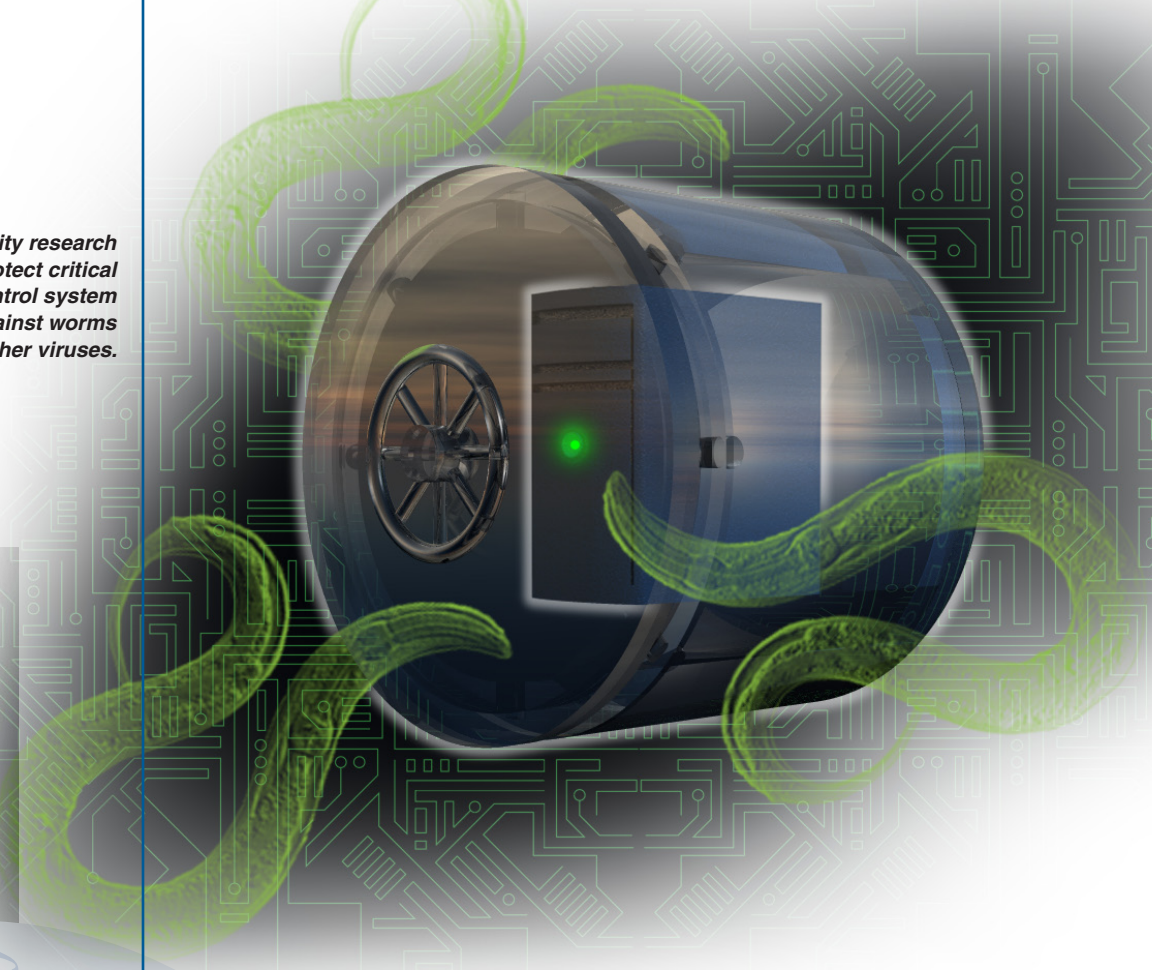
Access Denied



Cyber security research at INL will help protect critical infrastructure control system computers against worms and other viruses.

INL Cyber Security Research

Defending the Network Against Hackers

Network Interconnectivity

The business world is online. So are hackers.

The dangers and complications of controlling corporate network access and information flow from unauthorized users has been a consistent problem since the Internet's inception. The guiding principal seems to be that if a programmer can build it, a hacker can destroy it. A virtual back and forth battle of patches and worms, upgrades and viruses has evolved. In addition, the essential networks of control systems – those systems that operate our nation's critical infrastructures – such as electrical power grids, oil and gas refineries, and telecommunication systems, have been neglected in the realm of Internet security protection.

Many industries have not placed adequate emphasis on securing these systems beyond a standard firewall because traditional hackers had been more interested in exploiting large-scale, iconic targets such as government agencies and Fortune 500 companies. That changed after 9/11, when the federal government realized the motivation for terrorist attacks against the United States was

Continued next page

The Energy of Innovation

INL Idaho National Laboratory

Continued from previous page

to destroy economic stability and endanger public safety.

As stated by the Government Accountability Office, the threat posed by cyber attacks could have significant consequences to public health and safety. The reality that a malicious hacker, cyber terrorist or disgruntled employee could penetrate and damage any number of infrastructures with little more than a laptop and an internet connection, has become a serious security issue.

To combat this threat, the U.S. departments of Homeland Security and Energy selected Idaho National Laboratory to lead the nation in securing critical infrastructures and reducing the cyber vulnerabilities associated with control systems. A major objective to reducing the cyber threat to infrastructures is the research and tool development that takes place within INL's Cyber Security Research Department. To help support the Department, INL has constructed a comprehensive Cyber Security Test Bed. A test bed is a functioning model of full or near full-scale proportions that allows individuals to visualize, analyze and test their control systems in a domain that is more realistic than computer simulation.

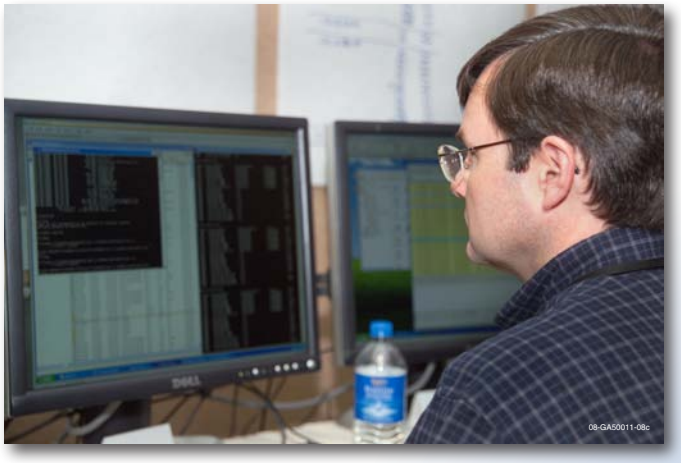
INL's Cyber Security Test Bed allows researchers to combat threats to the nation's critical infrastructures by creating an environment where tool development and simulated control system attacks can occur. Our cyber security researchers also provide security assessments and support to the National SCADA Test Bed, a multi-laboratory effort to reduce the vulnerabilities associated with supervisory control and data acquisition systems.

Securing the Network

According to the FBI, terrorists, transnational criminals and intelligence services are quickly becoming aware of and using information exploitation tools such as computer viruses, Trojan horses, worms, logic bombs and eavesdropping sniffers that can destroy, intercept, degrade the integrity of, or deny access to data. Using many of the same methods that malicious hackers would use, our cyber security

INL's Cyber Security Test Bed contains specialized equipment that can analyze and test a number of control system components.

Two INL cyber security researchers discuss the software coding of a computer virus in this photo taken at the INL's Control System Security and Test Center.



Cyber and control system experts at INL routinely perform comprehensive vulnerability assessments on vendor equipment and third-party products.

researchers identify control system vulnerabilities and provide analysis and assessment for improvement to utility companies and vendors. With previous clients, each system we have tested has been susceptible and vulnerable to probes and attacks from malicious hackers and virus writers.

The INL Cyber Security Test Bed is the only testing facility of its kind located within a national laboratory. The test bed gives customers access to multiple classified and unclassified test facilities and Critical Infrastructure Test Range components. Researchers are capable of providing a customized intrusion detection system, vulnerability assessment and exploit and mitigation development. Employees have informal relationships with international security resources.

Within INL's Cyber Security Test Bed we have the flexibility to replicate any customer's control system specifications. We can use those specifications to run simultaneous attacks on multiple systems, or we can perform individualized full-scale cyber attacks, in a controlled setting, on an exact replica system. In the future, the Cyber Security Test Bed will be capable of connecting to any number of related test beds located at the site in our full-scale Critical Infrastructure Test Range. This includes:

- SCADA Test Bed
- Power Grid Test Bed
- Mock Chemical Mixing Facility
- Wireless Test Bed
- Physical Security Test Bed

INL Cyber Security Test Bed has incorporated Virtual Private Network (VPN) connectivity to increase resource and testing capabilities. These VPNs allow access to databases and communities of control system specialists across the nation at other national laboratories and universities.

How We Can Help

Situated on 890 square miles of isolated landscape, INL has built and relied on our own control systems for more than 50 years. Our immense location requires us to operate and maintain a vast network of control systems for electrical, water and telecommunication distribution. Using this existing setup and our system expertise, INL is able to utilize our infrastructure as a full scale testing facility

Continued next page

Continued from previous page

to perform real world control system tests and attacks. Our goal is to significantly reduce the vulnerabilities associated with these systems.

Due to the sensitive nature of our work and findings, we use a number of different methods to secure customer data and vulnerabilities. We use both non-disclosure agreement and cooperative research and development agreements to protect customer information, vulnerability findings and suggested solutions.

Cyber Security Methods

INL cyber security researchers leverage the methods and ideologies that cyber terrorist and hackers possess so we can instruct our customers to protect themselves, their business and their stakeholders who depend on efficient, reliable and secure control system and network operation. The department works with a broad range of industries and vendors to develop mitigation techniques and tools, supported by out vast infrastructure Test Range, to reduce the cyber vulnerabilities found in many of the nation's critical infrastructures.

INL has established cooperative research agreements and non-disclosure agreements with dozens of companies, and is working with others that have expressed interest in the lab's capabilities.

For more information

Derek Hesse
(208) 526-9405
Derek.Hesse@inl.gov

Tom Anderson
(208) 526-2653
Thomas.Anderson@inl.gov

A U.S. Department of Energy National Laboratory

The Cyber Threat

- In 2004, the Pentagon cited sources that point to the development of an information warfare program in both China and North Korea.
- According to the United States Computer Emergency Readiness Team, or US CERT, as much as 80 percent of actual security incidents go unreported.
- The 2003 Deloitte and Touche's Global Security Survey found that 90% of computer security breaches originated from the outside.
- According to the Government Accountability Office, in 2002, 70% of energy and power companies experienced some kind of severe cyber attack to either their IT or SCADA/EMS network.