Stacking the Network Against Hackers

Cyber Security

Protecting computers and communications and the systems they link

Top-Notch Operations Experience

INEEL maintains multiple layers of firewalls, intrusion detection systems, hybrid systems, and encryption links for unclassified network operating centers, classified environments, and geographically distributed high-speed scientific networks. Our personnel have experience with and access to the latest information on hacker methods and defense techniques, and perform vulnerability assessments for other national laboratories, federal agencies, and commercial companies. INEEL experts are certified in multiple areas under the System Administration Networking & Security Institute's Global Incident Analysis Center training program.

Cutting-Edge, Practical Research

We are developing new software for distributed intrusion detection system modules that improve recognition of security attacks and forward critical alarms to centralized Network Operations Centers. We are also conducting research into survivable systems, cooperative agents, digital signatures, and secure communications protocols for both Department of Defense and Department of Energy customers. Through the Information Security and Reliable Computing Alliance, INEEL researchers cooperate with regional universities, including two that are certified by the National Security Agency for advanced computer and network security related research.

Large-Scale, Complex Integration

Public Key Infrastructure (PKI), Smart Cards and Digital Signatures

INEEL employees have extensive expertise in deploying enterprise PKI systems that use cryptographic smart cards similar to those used in Europe and by the DoD. Our researchers have developed and deployed a new digital signature system that extends Internet standard signature capabilities to complex objects stored in distributed databases instead of just a single "flat-file." This technology is the winner of 2001 White House award.

INEEL Idaho National Engineering and Environmental Laboratory
Home of Science and Engineering Solutions

The INEEL's extensive network test laboratory offers a wide range of training and hardware/software test capabilities.

Network Test Laboratories

The INEEL has an extensive network test laboratory that can be used for training, equipment testing, production simulations and trouble shooting, new release upgrade testing, network software testing, and beta testing. The primary test lab has Sun workstations and PC systems to test different areas of the network hardware configuration. Additional test setups include Novell IntraNetware, Windows NT/2000 servers, and end-node component testing.

The test bed is also used to test/mock up ATM (Asynchronous Transfer Mode), Wireless, T1, 10MB, 100MB and gigabit Ethernet networks alone or in various combinations. Video and data have been tested over some of these combinations. INEEL periodically acts as a beta test site for Cisco network equipment. Future upgrades to INEEL's networks include the use of Dense Wavelength Division Multiplexing (DWDM) technology that sends multiple wavelengths through the fiber to increase overall bandwidth or to partition/isolate services by wavelength. INEEL is doing controlled live tests for half a dozen DWDM venders on portions of INEEL's OC-3/OC-12 production fiber loops.

The INEEL's existing network development laboratory consists of almost 100 dedicated components staged in controlled access, with several separate raised-floor areas that are isolated from the INEEL production network. The network test lab can run entirely isolated or connected to external networks (Internet, ESNet, DOEnet, etc.) in a controlled fashion using multiple transport technologies. At any time these systems can be configured to allow real-time testing of new technologies without danger of impacting the mainstream user populace. Solaris, Linux, and several Windows variants are currently loaded on SUN, Compaq, and Dell platforms. These systems can be connected in both switched and routed configurations via ATM, 10 MB and 100 MB Ethernet connections including several router, firewall and intrusion detection system configurations. This test environment has hosted Cisco early field test activities for three years and is slated for a cooperative effort with DOE's Computer Incident Advisory Capability regarding the development of an ATM compatible network intrusion detection devices.

Testing Support - New Topologies and Technologies:

The INEEL has developed an isolated network that can be used to configure and simulate existing networks. This network can then be attacked looking for vulnerabilities and weaknesses, which once discovered can be used to repair the simulated network. Furthermore the testing can exercise new technologies, configurations, and evaluate performance while assuring that the simulated network remains protected. The network has two modes: one protected for experimentation, and the other highly interconnected for more distributed activities.

INEEL Network Testbed (INT)

Our objective is to provide access to and expand our existing Network Development Laboratory to other organizations, install or simulate their network features (software and hardware), and test for vulnerabilities. This enhanced INEEL Network Testbed is a highly flexible environment containing routers, gateways, switches, and processors that can be used to simulate and run various network configurations. Because it is isolated from the existing networks, white hat, red hat and black hat attacks can be made in a benign environment. In the interconnected mode, network interaction and further distributed activities can be conducted. The INT also can be used to investigate research in new and advanced network protection schemes.

Our computer scientists are developing tools through research, analysis, and simulation to determine network health, respond to suspected intrusions, and take steps to safeguard network assets. Technologies that can be used in this environment include artificial intelligence, fuzzy logic, adaptive agents, neural networks, fault tolerant techniques, dynamic network coalitions, non-repudiation of information, steganography, pattern recognition, and statistical analysis. INT provides a very dynamic environment that continually looks for problems and probabilistically determines the next actions to take, gathering more or different data, launching adaptive elements to combat problems in subnets, isolation of subnets, insuring that data collected is of forensic quality.

National SCADA Testbed

The INEEL – in partnership with Sandia National Laboratories – has established the National SCADA Testbed that combines efforts in security administration and governance, standards, industry alliances, education and awareness, modeling, vulnerability assessment of U.S. utilities, and research and development. The SCADA Testbed will also align with Homeland Security activities in physical security, certification and system reliability of energy infrastructure.

Information Assurance / Cyber Security

Our personnel are skilled in cyber security policy development, and day-to-day network operational security and have certified experience as network intrusion specialists. This expertise is augmented with the Laboratory and the University of Idaho's research and development capabilities. INEEL capabilities include:

•Automated war dialer – illicit modems

•Network Intrusion Detection

•Network security consulting

•Automated configuration scanning

•System administration (Sun, HP, Linux, Windows)

•DMZ Management

•Digital Signature plug-ins for web browsers

•Security and web-based training

•Procedures and checkouts for laptops used in sensitive travel

The INEEL also conducts research in:

Information Assurance
- insures that information is original

Intrusion Protection
- protection from attacks

Information Forensics
- investigation of suspicious situations

System Recovery
- protecting a system during and after an attack

•Snort – Open System Network Sensor / Intrusion Detection System

•Independent Verification and Validation

•Firewalls and Virtual Private Networks

•Public Key Infrastructure

•Work flow using digital signatures

•Penetration Testing (Internal and External)

•Vulnerability analysis and port scanning

•Digital signatures for relational databases

•Threat assessment procedures

Consultation

The INEEL is a cyber security consultant to the Bechtel Corporation and the Global Network Operations Security Center, which is part of the Defense Information Systems Agency and protects DoD networks around the world. INEEL is also a consultant for DOE's "Information Management and Correlation" system, which analyzes wide area network intrusion information.

These and other focused security activities lead DOE's Security Audit Team to call INEEL's performance "superb" in a recent security audit of INEEL operations. The INEEL was the first DOE laboratory to successfully pass this comprehensive audit upon initial review, and received recognition for two best practices.

For more information:

Wayne Austad
(208)526-5423
wqa@inel.gov

Rob Hoffman
(208) 526-8599
hoffrw@inel.gov

Gary Seifert
(208) 526-9522
sei@inel.gov