Network analysis and cyber security lab

Introduction

In today's environment, it is essential to assure that networks are protected against the increasing frequency of malicious viruses, worms, hackers, and other types of attack. To integrate several ongoing research programs in this area, Argonne's Decision and Information Sciences Division established the Network Analysis and Cyber Security Lab. The lab provides the infrastructure, tools, and expertise for network analysis and security in support of federal agencies, military sponsors, and commercial organizations in their network design and operations.

Technical Capabilities

The Network Analysis and Cyber Security Lab and its staff provide a wealth of system, network, and security expertise in many areas. The following sections highlight activities that demonstrate our expertise.

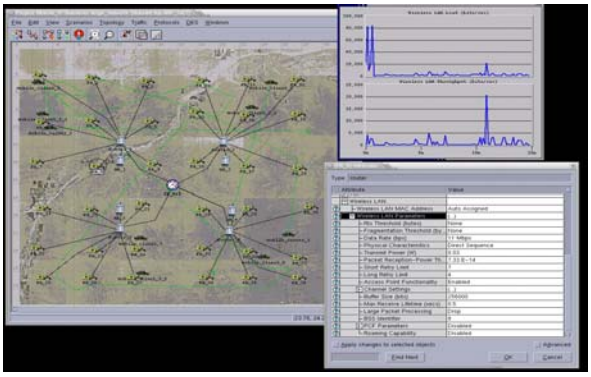
System and network security. Our staff operates large-scale integrated Windows, Mac, and UNIX networks and data acquisition systems for Argonne and government agencies. Our experts in security technologies help protect systems or networks from attack.

Networks for scientific data acquisition. For the Department of Energy's Atmospheric Radiation Measurement (ARM) Program, our staff designed and implemented a large-scale network for data acquisition. Through this network, weather data are collected from remote sites worldwide by using network technologies and satellite communication systems.

Network security test bed. To allow experimentation with technologies, the lab established isolated networks and plans to work closely with government agencies and industry to assess, evaluate, and test technologies for network security.

Large-scale data mining for security applications. The lab's staff has been involved in large-scale data mining of security audit logs and Web logs. This effort allows us to determine the origins of inquiries, patterns of access, and general data discovery from this tracked information.

Network analysis. Our staff has used commercial network design and analysis technologies (e.g., Opnet), to examine fielded networks for traffic analysis, performance, and architecture validation.



Network analysis tools

Vulnerability assessments/penetration testing. The lab has helped conduct vulnerability assessments and "white hat" penetration testing of government and energy-related industry systems.

Sensor integration networks (Biological Warning and Incident Characterization Program and PROTECT). The lab has integrated distributed chemical-biological sensor systems in secured networks to provide warnings and applied this technology to subway systems, national events, and urban environmental monitoring. These automated hardware and software systems integrate sensors, closed-circuit television, dispersion modeling, and optimal response protocols to improve detection of agents.

PROTECT warning system

SCADA. Supervisory control and data acquisition (SCADA) systems are used widely in industry (e.g., gas, oil, electric, water) to monitor and control remote equipment from a central facility. The lab has SCADA subject-matter experts from industry and has assisted DOE in determining best practice guidelines for SCADA equipment.

Certification and accreditation (C&A). Our staff has extensive experience in conducting C&A assessments of systems, including preparing documentation and performing testing on these systems (security test and evaluation). This expertise extends to FISMA and A123 assessments. Tools are being developed to assist in collecting and organizing the massive amounts of data required in these assessments.

Secure computing. The lab provides a secure computing facility for classified work. Diskless workstations provide project-specific information access. Our staff is familiar with Sensitive Compartmented Information Facility (SCIF) design, security requirements, and operations.

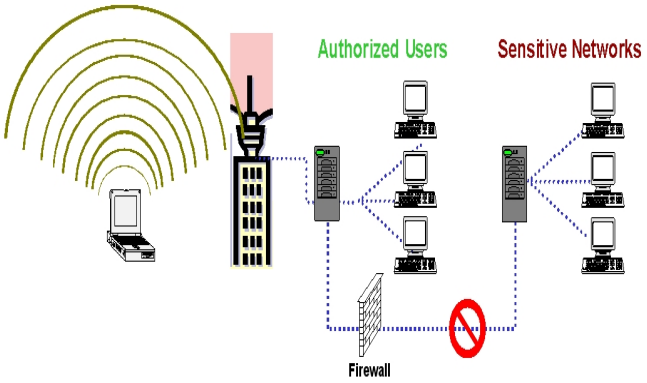
Independent verification and validation (IV&V). Our staff has extensive experience with IV&V of large-scale government and international treaty systems. Our unique experience with IEEE standards and methodologies for testing complex systems provides an established, dedicated network for testing.

Wireless communication technology. The lab has researched and prototyped wireless networks for data and video in connection with a sensor that is deployed in a subway warning system.

Globus security for database access. For this project, our staff developed a unique approach for implementing end-to-end security for database access. We eliminated the need for security controls at the middleware layer and provided security directly from the client to the database on a Globus network.

Intrusion detection systems (IDSs). Staff members assessed and evaluated existing commercial and government IDSs and their extensions. Coordinated IDSs, which use multiple technologies on large-scale networks, "vote" on the existence and nature of an attack, leveraging the unique features of each IDS and reducing the number of false positives. The sharing of information between IDSs can identify coordinated attacks and can be used to prevent attacks on other systems.

Installation infrastructure modernization. Staff members are assisting the U.S. Army with the implementation of the Installation Information Infrastructure Modernization Plan and transition to an Area Processing Center by providing independent evaluation and assessment of transition plans.



Wireless secure networks

Learn more about network analysis and cyber security at:
http://www.dis.anl.gov/exp/IS

For more information, contact:

Craig Swietlik, Group Leader
Information Sciences
Decision and Information Sciences Division
Argonne National Laboratory
9700 S. Cass Avenue, Bldg. 900
Argonne, IL 60439, USA
630-252-8912 or swietlik@anl.gov

October 2008

A U.S. Department of Energy laboratory
managed by Uchicago Argonne, LLC