I4 Information and Infrastructure Integrity Initiative

I4 Newsletter – Winter 2009

Mission

The Information and Infrastructure Integrity Initiative mission is to define, develop, and validate a new proactive-predictive-adaptive strategy that will enable information infrastructure operators to anticipate and adaptively respond to attacks in real time and to prevent loss of information integrity.

Initiative Team

Initiative Lead: Deb Frincke
Deputy Lead: Gary Morgan
Science Advisor: Jim Thomas
Adaptive Systems Focus Lead: Glenn Fink
Predictive Defense Focus Lead: Frank Greitzer
Client Outreach: Troy Thompson
Operations: Tim Strycker
Administration: Kim Deitchler
Communications: Janine Anderson
Financial: Nancy Smet

http://i4.pnl.gov

For more information, contact: Deb Frincke
Phone: (509) 375-3969
Email: deborah.frincke@pnl.gov

Pacific Northwest NATIONAL LABORATORY

Proudly Operated by Battelle *Since 1965*

Deb's Thoughts

2009 – what challenges! Cybersecurity is on everyone's list of concerns and visionary solutions are clearly needed. Yet, our nation's other challenges and the urgent need to address existing cyber threats tempt us to stick with "catch-n-patch" solutions that increasingly fail us today. To be relevant in this climate, we must balance our scientific achievements with the need for rapid solutions. This inaugural edition of the I4 newsletter provides a sampler of PNNL investments in research, partnerships, and infrastructure necessary to advance the "safer and more secure" infrastructures required for our national security, energy solutions, and scientific collaboration.

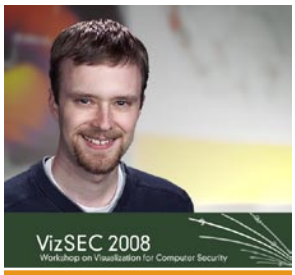
Partnering with CIAC and UW

Pacific Northwest National Laboratory's (PNNL's) scientific partnership with the Center for Information Assurance and Cybersecurity (CIAC) at the University of Washington (UW) has secured their spot as one of the first centers in the United States to be designated as a National Center of Academic Excellence in Information Assurance Research (CAE-R) by the National Security Agency and the Department of Homeland Security (DHS).

For more than three years, PNNL has assisted CIAC on a number of projects from a joint research effort funded by the U.S. Department of Energy (DOE) that included UW researchers to educational programs such as lectures on cyber security and advanced forensics.

The Center will be a forum for the collaboration of professors, professionals, industries, and students to identify, address, and promote visions and solutions for issues of information assurance and cyber security. The focus of the Center will be on research, invention, innovation, education, public awareness, entrepreneurship, and economic growth in the state of Washington, which will assist with sustaining the vitality of existing industry as well as attract and develop new industry.

Mike Kluse, PNNL, Deb Frincke, PNNL, Barbara Endicott-Popovsky, CIAC-UW, Harry Bruce, iSchool, UW



Collaboration Corner

Bridging the gap between visualization and automation—that was the theme for the 5th annual VizSec workshop for Cyber Security, which was held in conjunction with RAID 2008 and where Jereme Haack presented a poster on Cooperative Infrastructure Defense (CID). The CID is a human and software agent solution that couples human intelligence with a hierarchy of rational software agents to cooperatively protect an infrastructure of independent organizations and agencies. Jereme stated that most people who stopped by the poster were interested in the approach and eager to see more publications about this technology.

About our focus areas

Our research approach in predictive and adaptive areas will advance the use of prediction and associated technologies such as models, simulations, and behavior analyses/predictions to better understand the potential effects of existing and emerging threats and vulnerabilities and develop ways to provide timely, self-managed responses with bounded consequences.

Predictive Defense

The main focus of predictive defense R&D is to develop innovative methods, analyze historical and current system information, and predict future states of information technology (IT) infrastructures/systems as well as identify potential threats, with the purpose of preventing or limiting the impact of attacks. The scope of the predictive defense focus area is to conduct research and development on cyber security/IT network defense and other complex networks such as the Internet and the electric power grid.

Adaptive Systems

The intent of the adaptive systems focus area is to investigate revolutionary technologies that will enable cyber systems to maintain a stable, secure state despite activities of attackers from both within and outside. The focus area includes adaptive tactics to respond to a changing environment (including attacker activity), self-healing systems, and adaptive machine-learning technologies whose goal is to understand the environment so it functions stably within it. The scope of this area is to conduct research and develop cyber security and network defense technologies, systems, and infrastructures and therefore protect complex, heterogeneous computer networks.

Project Update: Predictive Defense

PACMAN:IT Predictive Adaptive Classification Model for Analysis and Notification: Internal Threat

Key idea: Use of organizational (psychosocial) as well as IT/cyber data within a predictive modeling and analysis framework that improves situation awareness and filters/focuses security analyst's attention on possible higher-risk exploits by insiders.

The prototype system under development, called Psyber Sleuth™, implements a distinctive modeling approach that incorporates psychosocial data to extend the cyber security analyst's time horizon for proactive defense/mitigation of potential malicious exploits by insiders.

Managing Complexity of High Volume Predictive and Adaptive Network Operations

Key idea: Novel methods to predict possible future impacts of alternative courses of action (candidate corrective measures) by visualization and modeling of system/infrastructure data

The project handles a large volume of predictions using analytical methods to accomplish a three-step prediction process: prediction of 1) deteriorating conditions, 2) the consequence of the problems, and 3) the effect of remedial actions to significantly improve real-time operation of complex networks such as electric power grids.

CARIM

Key idea: Risk-based model as the basis for analysis of cyber activity to infer attack purpose and goals.

The purpose of this project is to create a risk-structured repository of attack scenarios and defensive measures based on I4 insights, elicitation from the external cyber community, and using the risk-based scenario repository as the basis to infer likely intent associated with real-time cyber data.

Project Update: Adaptive Systems

TDMAA Tactical Deployment and Management of Adaptive Agents

Key idea: Couple human intelligence with a hierarchy of rational software agents to cooperatively protect an infrastructure of independent organizations and agencies.

This project is a novel framework that enables cooperating organizations to mutually defend against cyber threats and support the awareness, prevention, and response functions to DHS.

MLSTONES Machine Learning String Tools for Operational and Network Security

Key idea: Exploit biosequence theory to provide rigorous and repeatable framework to augment cyber security.

This project is a collection of methods for characterizing text-based strings from various cyber applications using biological sequence analysis theory and machine learning to extract patterns. The purpose is to provide capability framework for rapidly developing new text-based characterization applications in cyber domains and to provide a pattern-matching approach to complement or augment current rule-based approaches in cyber security.

PNNL-SA-64525