I4 Information and Infrastructure Integrity Initiative

I4 Newsletter – Fall/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
Senior Research Leads: Glenn Fink, Frank Greitzer
Client Outreach: Troy Thompson
Operations: Tim Strycker
Finance: Jenny Oelerich
Communications: Janine Anderson, Keri Schneirla
Administration: Sherrie Bowers

http://i4.pnl.gov

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

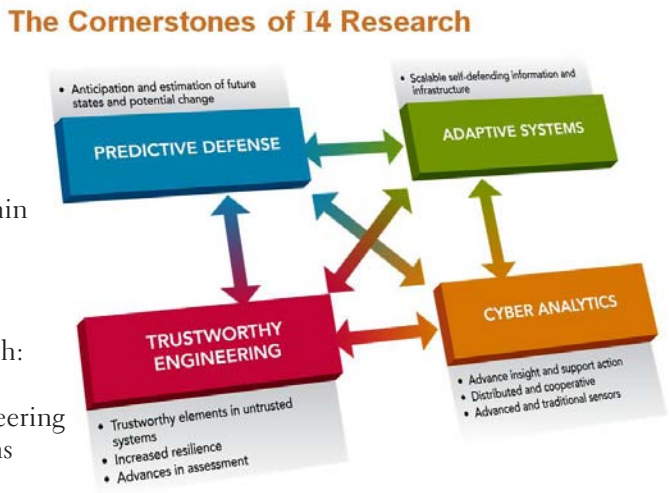
To learn more about I4, listen to Deb's podcast at:
http://www.govinfosecurity.com/podcasts.php?podcastID=271

Pacific Northwest NATIONAL LABORATORY

Proudly Operated by **Battelle** *Since 1965*

Deb's Thoughts

In our third year, the Information and Infrastructure Integrity Initiative (I4) continues to extend PNNL's research and development capabilities in the areas that include the resilience of large-scale digital computer and control infrastructures, the communications within those infrastructures, and the soundness of information contained/transported by the infrastructures.



Through the four cornerstones of research: Predictive Defense, Adaptive Systems, Cyber Analytics, and Trustworthy Engineering we are looking for solutions to our nations hard questions.

- National Security – Primary challenges are how can we predict the presence of potential vulnerabilities in complex infrastructures that are critical to energy and security missions, or the potential for damage when adversaries gain new capabilities?
- Energy – The primary challenge is how can the broad energy infrastructure be made even more self-securing, so it can react fast enough to remain resilient under cyber attack without triggering negative, unintended consequences?
- Open Science (collaborations involving multiple institutions and crossing national boundaries) – Primary challenges are how can we ensure that data integrity and site security are maintained while supporting information availability, and that neither sensitive nor protected information is inadvertently leaked?

Digital Ants featured on Discovery, MSNBC, and SmartPlanet

http://dsc.discovery.com
http://www.msnbc.msn.com
http://www.smartplanet.com

Partnering with Wake Forest University leads to a new methodology that is crawling with interest

Erin Fulp of Wake Forest and two of his graduate students spent last summer at PNNL working with Glenn Fink to code and test a solution to search out viruses, worms, and other malware based on an army of digital ants. The new solution could provide better protection while freeing up valuable hardware.

The way current anti-virals stand now, it's basically a game of cops and robbers. Firewalls stand at the entrance to a system, scanners conduct regular inspections—like cops raiding a joint with photos of the usual suspects. The problem though is that, just like the real world, bad guys disguise themselves. Many of the programs that do the most damage to computers and networks are classified as worms. They mimic animal behavior by copying themselves inside networks,

without human intervention. So, Glenn's idea was based around the thought of "why mimic the behavior of human cops and guards at all?" and that's where digital ants were born.

Rather than big programs that carry the equivalent of mug shots, the idea is to break the work down into smaller pieces and focus on maintaining safety, not catching crooks.

Fink, Fulp, and his team created four digital ants of the 64 types of conditions. They setup a bank of computers and released three worms into the ant-infested Linux-based computers. The four digital ants in the computers had never seen the viruses before, yet were able to identify the worms by only monitoring four very specific aspects of the computers.

Fulp describes the results as "swarm intelligence," likening it to ant behavior in nature. Ants swarm to anything that appears wrong and surrounds it, collecting data.

The key is that all these programs are small objects. You can deploy a lot of them when needed, cut their numbers when they're not, all under control of other software objects. Reports and commands to programmers are specific and action-oriented. The art of using digital ants, instead of traditional anti-virus programs, is their flexibility. Traditional anti-virus software usually scans constantly or on a set time schedule. Constantly scanning for threats is effective, but uses a lot of computer resources, resources that could be better spent doing something else.

I4 Project Focus

Managing Complexity of High-Volume Predictive and Adaptive Network Operations

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

PD-Smart Predictive Defense Model for the Smart Grid

Key idea: Develop a predictive defense model that identifies threat patterns, predicts threats, and takes action based on potential impacts on power grid reliability and stability to remove, prevent, or mitigate vulnerabilities.

CARIM Cyber Attack Risk Identification

Key idea: Implement a 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.

VULCAN Unexpressed Communication

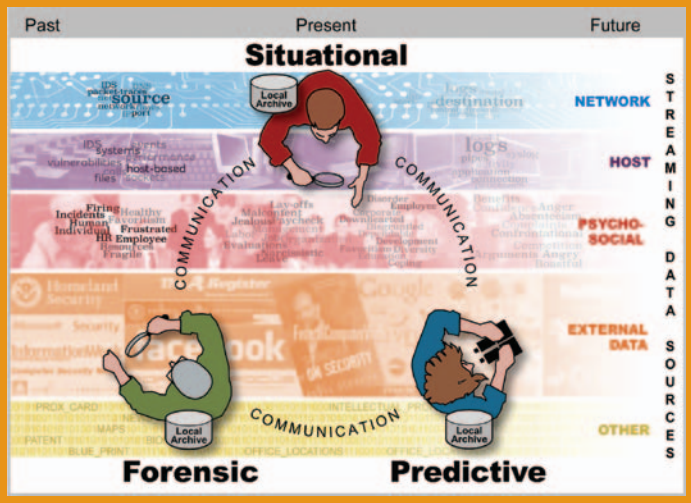
Key idea: This is a project that aims to fill the gap in communication and collaboration among cyber security analysts, both within an organization and across organizational and even national boundaries.

MLSTONES Machine Learning String Tools for Operational and Network Security

Key idea: This is a set of high-performance computational capabilities that uses inexact string-matching techniques from bioinformatics for applications in many different areas of cyber security, including software analysis, binary identification, network security, and photographic image comparison.

ACAMP Adaptive Cyberdefense using an Auto-associative Memory Paradigm

Key idea: Design, develop, and test an adaptive attack recognition system that transcends current approaches by employing an adaptive mechanism to recognize subtle variations on input data.

Cyber Analytics

Cyber analytics can be applied to many applications, but in PNNL's Secure Cyber Systems technical group, we are primarily concerned with improving the safety and soundness of our cyber systems and infrastructures through security technologies.