I4 Information and Infrastructure Integrity Initiative

I4 Newsletter – Spring/Summer 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

Welcome to this second edition of our I4 Newsletter.

This year continues to be a time of transition in technology as well as government, but the four corners of I4 research remain relevant. The intertwined themes of Predictive Defense (forethought supporting preventive measures) and Adaptive Systems (enabling rapid action) are joined by funded projects in Cyber Analytics, described in this edition. Associated with each of these three areas is the notion of Trustworthy Engineering–how to operate securely in an insecure world, how to operate resiliently in support of a mission, and how to verify/validate/assess results in a scientifically repeatable manner. Advances in any of these three areas will support improvements in the other three–improved analytics supports better predictions, improved predictions allow for better adaptations, and adaptation can result in improved resilience.

We are now selecting our new projects for 2010, and have identified several solid candidates who will be briefing our advisory board in June on their ideas. Numerous interns have also joined the initiative to work on our LDRDs. Also, we are welcoming a new PNNL hire, Dr. Thomas Carroll, who will be joining us very soon. Dr. Thomas Carroll recently completed his PhD at Wayne State University, with published papers combining security, game theory, and economics.

Cyber Analytics: The story behind cyber data

Cyber analytics—one of the four cornerstones of the Information and Infrastructure Integrity Initiative—is the science of analysis as it relates to people, computers, and infrastructures. It uses PNNL's existing capability in decision-making and information-gathering as applied to cyber-security systems to support both better predictions and guide adaptive responses of the infrastructures. Our primary investments in Cyber Analytics will emphasize distributed approaches–distributed in both data sources and the analysts who will use them.

Cyber Analytics research is an important contributing element to both predictive defense and adaptive approaches. Better Cyber Analytics will improve defenders' situational awareness and help analysts respond proactively,

I4 Career Opportunities – Want to change the world?

Are you interested in providing research leadership involving Information and infrastructure and integrity? If so, visit our website to learn more about the opportunities.

http://i4.pnl.gov/recruiting.stm

Kudos to Henry Huang

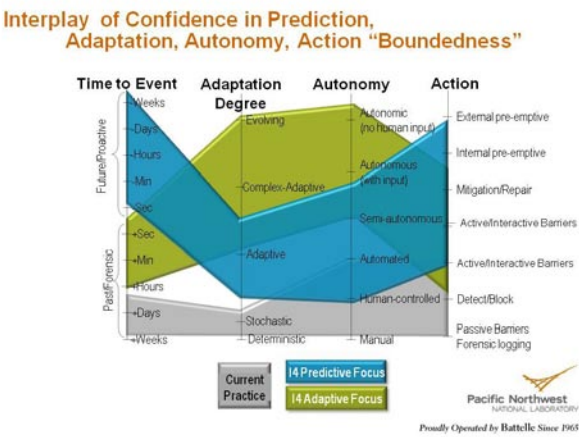
Henry Huang will receive the 2009 Institute of Electrical and Electronics Engineers (IEEE) Power & Energy Society (PES) Outstanding Young Engineer Award. The award recognizes engineers 35 years of age or under "… for outstanding contributions in the leadership of technical society activities, including local and/or transnational PES and other technical societies, leadership in community and humanitarian activities, and evidence of technical competence through significant engineering achievements." As a recipient, Henry will designate a college or university to receive a $2,000 electrical engineering scholarship from the Society. He is scheduled to accept this award at the awards luncheon July 28 at the IEEE PES General Meeting in Calgary, Alberta. Congratulations on this achievement, Henry!

or at least in a timely manner. Adaptive systems also benefit from improved analytics–and a key research challenge will be how to provide the insights needed to support effective human-guided and automated responses. Large-scale distributed collaboration in cyber defense will require very broad, nontraditional command and control strategies; significant research remains to be done in this area. Finally, defenders need to learn to use deception and to detect deception by attackers. This is another area in which I4 investments may have an impact.

Bottom line—Cyber Analytics tells the story behind cyber data. There are potentially many stories, depending on the purposes and perspective of the analyst. Our Cyber Analysts strive to address these areas and gain the understanding needed to develop capabilities that support predictions and guide adaptive responses of the infrastructure. For more information, contact Glenn Fink at glenn.fink@pnl.gov.

Working together

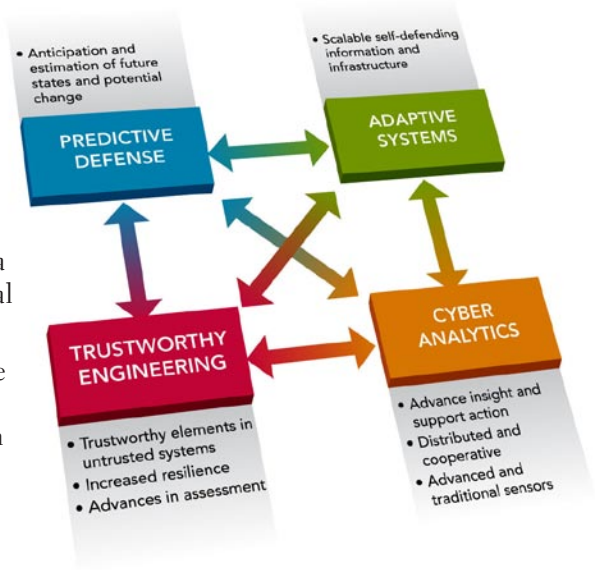
A key element of I4 is the interactions among the four characteristics, in particular, the interactions among Predictive Defense and Adaptive Systems. We consider four characteristics to encompass the "playing field": Time to Event, Adaptation Degree, Autonomy, and Action. Activities that anticipate attacker actions are Proactive, while those that examine or remedy what happened previously are Forensic. The goal of Predictive Defense is to allow higher confidence actions to take place earlier in the cycle of attack/defense. This is represented in the Time to Event axis. Adaptation identifies the degree to which a cyber defense can change, while Autonomy describes the amount of freedom a system can be provided without human supervision. The Action section describes a range of more (or less) extreme measures that might be taken. Those that would be acceptable will depend greatly on the confidence with which an event is predicted, how much flexibility the responding system has, and the degree of autonomy that the acting system will have.



The green area in the graph illustrates modern cyber-security systems, which concentrate on forensic detection with very little adaptation or autonomy. Reasonable actions for such a system could span the gamut–but they would require rigid control. In contrast, the Predictive Defense approach supports proactively solving threats, both by perceiving and acting on them earlier. These defenses will be able to adapt to changes in their environment and will have much greater freedom to act than existing systems. However, because they are predictive in nature, we would expect that human intervention would be needed if actions are taken outside the boundaries of the system being defended. Similarly, the Adaptive Systems focus area seeks to bring greater flexibility and autonomy to cyber-defensive systems. We anticipate adaptive systems that will be able to predict imminent changes in attack tactics and adapt to them before attackers can.

The cornerstones of our research

Our goal is to establish PNNL as the recognized leader in innovative and proactive science and technology to prevent and counter acts of terroris, or malice intended to disrupt the nation's digital infrastructures resulting in a safer and more secure digital infrastructure.



To accomplish this goal, the I4 science and technology agenda is advanced through core cornerstone concepts and architecture for combining them.

1. Predictive Defense. Our research approach advances the use of prediction through use of models, simulations, and behavior analyses to better understand the potential effects of existing and emerging threats and vulnerabilities, and to use these insights to prepare systems so that they will be capable of preventing failure, or proactively mitigate the actions of attackers.
2. Adaptation is employed to improve the timeliness of responses, as well as to allow independent, albeit bounded, responses to changing requirements and threats, and as a preventative measure. Through Adaptive Systems research, we can provide more resilient systems.
3. Cyber Analytics research supports improved situational awareness, and also addresses the needs of modern analysts, who may be geographically and organizationally distributed, yet need to collaborate to achieve common goals.
4. In 2010, we hope to begin investments in Trustworthy Engineering. Trustworthy engineering is intended to support operation in "The Real World," where systems are often partially compromised or breakable, stakeholders have conflicting goals, users are mobile, and effective yet practical solutions are needed.