Dear I3P Colleagues,

I wanted to write a quick note as we rapidly approach the I3P’s 10th anniversary. The consortium has brought together some of the best minds in cyber security, in collaboration with our sponsors and end-users. We have developed products and offered insights that have reduced the overall risks to critical infrastructure, while mentoring and developing a new generation of researchers to follow our path.

At the same time I3P has led discussions of infrastructure resilience, our consortium has also shown quite a bit of resilience, and flexibility, as our research and funding models have evolved to fit the ever changing climate and appetite for research. From project selections competing for portions of a dedicated grant, we have developed a strong portfolio of sponsors and initiatives. I want to thank Dartmouth both for the leadership it has provided and the continued belief that Dartmouth’s investment in I3P adds meaningful value for critical infrastructure protection.

Our new model demands more from each of us and of our institutions, but we are ready for those new responsibilities. I look forward to working with you all for the next ten years, and beyond, as we develop an ever stronger consortium and address the cybersecurity issues of the future.

—Zach Tudor, I3P Executive Committee

I3P Welcomes New Members to the Consortium

For the first time in over five years, the I3P has offered membership to three new institutions. Binghamton University, George Washington University, and Oak Ridge National Laboratory have joined the 25 other member institutions that constitute the I3P as we work to strengthen the cyber infrastructure. Each of the new institutions brings a unique perspective to cyber security, and its representatives will add value to our multidisciplinary approach.

Kartik Gopalan is an Associate Professor at Binghamton University and its new primary representative to the I3P. A Ph.D. graduate of Stony Brook University, his current research focuses on resource virtualization and security in cloud computing and distributed systems. He is a recipient of the National Science Foundation CAREER Award and holds three US patents related to cluster-wide memory virtualization.

Binghamton University has a well-established program in security research that ranges from trustworthy cloud computing and information flow security to steganography, forensics, and malicious code detection. Binghamton offers security education across multiple departments at both undergraduate and graduate levels.
CSIRT

...continued from page 1

Over the course of three years, the team will review CSIRT guidelines already available from other organizations, and then observe and analyze current CSIRT activities at the Navy and Marine Corps Intranet, the largest internal computer network in the world. By studying documentation, observing behavior and conducting interviews, the I3P team will make recommendations for effective CSIRT formation and sustainment, and compare them to current strategies. The recommendations will be vetted using incident simulations, extrapolating the results in a variety of operational models. The project's goal is to learn how to best create, manage, and sustain an effective CSIRT; as with other I3P projects, the results will be transferred in publications and presentations that can easily be applied to commercial use. Near the end of the project, a CISO workshop will be held to disseminate the team's findings.

I3P’s Tackles Usable Security in New Project

The I3P has begun work on a project focused on usable security; a multi-institutional endeavor leveraging the breadth of expertise within the consortium.

The Usable Security project team aims to increase the presence and importance of security in all stages of software development rather than something tacked on as an afterthought. Sponsored by the Department of Homeland Security and the National Institute of Standards and Technology, the project brings together researchers from the MITRE Corporation, George Mason University, and Sandia National Laboratories. Also working on the project is the I3P’s research director, Shari Lawrence Pfleeger, and University College London’s Angela Sasse. The project was developed as a result of an I3P- and NIST-sponsored workshop examining the challenge of integrating security and usability into the design and development of software.

Over the course of the project, the team will conduct case studies of usable security design and implementation for use in understanding the problems and in teaching developers about solutions.

New Members

...continued from page 1

George Washington University’s (GW) primary representative to the I3P is Professor Lance Hoffman, Distinguished Research Professor of Computer Science and the Director of the Cyber Security Policy and Research Institute at GW. Author and editor of numerous articles and five books on computer security and privacy, he directs the computer security “Cyber Corps” scholarship programs at GW.

Professor Hoffman developed the first regularly offered course on computer security at the University of California, Berkeley in 1970 after serving on the Advisory Committee to the California Assembly Committee on Statewide Information Policy. A Fellow of the Association for Computing Machinery, Dr. Hoffman institutionalized the ACM Conference on Computers, Freedom, and Privacy in 1992, and has served on a number of Advisory Committees including those of Federal Trade Commission, the Department of Homeland Security, the Center for Democracy and Technology, and IBM. He received his Ph.D. from Stanford University.

George Washington University is a federal Center for Academic Excellence in Information Assurance Education and Research. It has produced graduates at the bachelor’s, master’s, and doctoral levels specializing in computer security and information assurance from a number of its departments, including Computer Science, Forensic Sciences, Public Policy, Electrical and Computer Engineering, Business Administration, Information Systems Technology, International Science and Technology Policy, and Engineering Management and Systems Engineering. This Fall, it began offering a new master’s degree of cyber security in computer science.

Another national laboratory has joined the I3P as a new member. Oak Ridge National Laboratory (ORNL) will be represented by Richard Linger, a Senior Cyber Security
Canegie Mellon University's Alessandro Acquisti warns of the privacy risks associated with biometric proliferation.

- Mercury News

• Quantum Information Sciences: Development of quantum building block for transformational technologies in cyberspace.

Key CSIIR R&D initiatives include automated software behavior computation, embedded device security, ultra-secure communication and authentication, and establishment of a national malware repository.

The I3P is pleased to welcome these three institutions to the consortium and looks forward to their contributions to cyber security research. As the I3P scales its efforts to address growing problems in cyber security, the ability to leverage the expertise of our increasingly diverse pool of researchers will prove invaluable.

I3P Researchers in the News

Canegie Mellon University's Alessandro Acquisti warns of the privacy risks associated with biometric proliferation.

- Mercury News

Brian Teirney of Lawrence Berkeley National Laboratory explains his research on 100 Gbps networks in an interview with Jon Bashor of Berkeley Lab Computing Sciences Communications.

- HPC Wire

Dartmouth's Eric Johnson discusses the risks and benefits of electronic health records.

- Information Week

Sujeet Shenoi of the University of Tulsa speaks on the NSA's involvement in Cyber Corps, an academic program designed to train "cyberninjas."

- Fast Company

Deirdre Mulligan's concerns over privacy and unique identifiers in consumer devices are explored in an article on Apple's iOS.

- ACLU

To view these news articles and more, please visit: http://www.thei3p.org/news/researchersinthenews.html
Upcoming Events

October 10th, 2012
10 Year Anniversary Meeting
Washington, D.C.

March 18th-20th, 2013
7th IFIP Working Group 11.10 International Conference on Critical Infrastructure Protection
Washington, D.C.

For more information on these and other events, visit http://www.thei3p.org/events/

For more information, contact kiel.h.alarcon@dartmouth.edu
To subscribe or unsubscribe send an email to kiel.h.alarcon@dartmouth.edu with the subject line “Add/Remove I3P Newsletter Subscription”