Message from the Executive Director

The release on May 29th of the President’s long-awaited Cyberspace Policy Review brings our nation’s cyber security challenges into sharp focus. Thorough, thoughtful and timely, the document speaks to the urgent need to secure cyberspace and to move ahead in a collaborative fashion. The fact that the President has publicly committed significant attention and resources to this issue is welcome news.

We are heartened to see the I3P report National Cyber Security Research and Development Challenges* mentioned in the President’s Review and to learn that, of the 22 academic institutions asked to provide input, 13 are I3P member institutions.

We are also pleased to see the attention the President’s Review gives to cyber security research and development. Support for research and development, which will ensure the Nation’s continued ability to compete in the information age economy, has a prominent place on the Review’s list of action items. In addition, the document explicitly states that the academic and cyber security research community is integral to the nation’s efforts to design, build and deploy trustworthy systems.

The President’s Review describes yet another finding that was underscored in the I3P report: the need for the public and private sectors to work together. Collaboration is not only imbedded in our mission statement but has defined our work for the past seven years. Each of our projects engages stakeholders and end-users throughout the research process, drawing on their input, and incorporating technology transfer into the planning process.

At the I3P we will continue to apply our multidisciplinary, multi-institutional approach to cyber security research and will work with the Administration, as well as our sponsors, collaborators and stakeholders, to push innovation and game-changing technologies. Only by partnering in this way can we help to ensure the security, reliability, trustworthiness and resilience of the nation’s information infrastructure.

--Martha Austin, Executive Director

I3P Announces Postdoctoral Fellows

The I3P has selected two postdoctoral fellows for the upcoming 2009–2010 academic year: Earl Barr, of the University of California, Davis, and David Dagon of the Georgia Institute of Technology.

Now in its sixth year, the I3P Fellowship program enables recent Ph.D. recipients to spend a year conducting cyber security research at an I3P member institution. “Mentoring the next generation of cyber security experts by pairing gifted young researchers with preeminent faculty at I3P institutions has a tangible impact on cyber security education in the U.S.” says Charles C. Palmer, the I3P’s Director for Research.

I3P Fellows benefit from expanded research breadth, as they work with new advisors and institutions and move on after their fellowship year to prestigious university and industry jobs. Although Barr and Dagon will remain at their respective graduate institutions, they will broaden their research and be mentored by new advisors.

Under the tutelage of UC Davis professor Zhendong Su, Barr will study obfuscation engines: programs that transform human readable code into indecipherable or hidden code. Obfuscation techniques have both legitimate and nefarious applications. Barr...

...Continued on page 2

Peter Neumann Delivers Keynote on e-Healthcare

In April 2009, the National Institute of Standards and Technology, better known as NIST, hosted a gathering of information security experts to address identity and trust on the Internet.

I3P researcher Peter Neumann, principal scientist in the Computer Science Lab at SRI International, delivered the keynote talk at the ID Trust 2009 meeting, urging the audience to consider not just trust, which is human dependent, but also trustworthiness when tackling the challenges of secure computing. Trustworthiness, he proclaimed, is especially critical in the healthcare sector, where electronic records are rapidly replacing paper files, and in many other application areas such as critical national infrastructures.

...Continued on page 2

will examine each, performing cost/benefit analyses from the perspectives of both the obfuscator and the de-obfuscator. If, for example, an obfuscation engine injects excessive junk code, the malware will become too large to be viable, resulting in a cost to the obfuscator. In contrast, the effort required to decipher the obfuscated code determines the cost to the de-obfuscator. Drawing analogies to game theory, Barr notes that, “obfuscation techniques drive the malware arms race,” so he wants to understand “the best moves for each player in the game.”

Dagon’s research will focus on the Domain Name System (DNS), the method by which the names of online services are translated into numerical addresses for proper routing. The DNS acts as “a directory service for the cyber world,” explained Dagon’s advisor, Mustaque Ahamad, Professor and Director of Georgia Tech’s Information Security Center, changing human-entered urls into computer-readable IP addresses (e.g. www.dartmouth.edu becomes 129.170.20.25). When a system is compromised, information can be intercepted. An analogy is “making a sensitive phone call to a trusted party, but having the message instead go to a rogue party,” said Ahamad.

Although secure versions of the DNS are being developed, they will take years to deploy, so Dagon hopes to develop interim solutions. As a “leader in the DNS security area [Dagon will] utilize the significant relationships he has with major stakeholders,” says Ahamad, “to assess real attacks along with possible counter measures.”

Ronald Dodge, Chair of the I3P Fellowship Committee and a professor at the United States Military Academy, says the work of these I3P fellows, like that of their predecessors in the program, “advances our security posture at a national level.”

Dagon and Barr were selected by a seven-member committee of I3P institutional representatives. Although the high caliber of proposals has remained constant throughout the award’s six-year history, the committee received a record-breaking number of applicants this year, said Dodge. For more information on the Postdoctoral Fellowship and other I3P educational initiatives, visit http://www.thei3p.org/education.

—in Bridget Alex, Dartmouth Class ’08

Peter Neumann

“In an era of increasingly depersonalized medical care, when more time is spent with computer records than with patients,” he said, “developing trustworthy systems is an imperative.”

But the challenges are daunting. Not only are reams of sensitive health data available online, but the technical requirements for e-healthcare range from identity verification for patients and staff, to access management for employees with shifting privileges, to network monitoring in a world awash with cybersecurity threats. A further complication is the sheer number of people, including administrators, healthcare providers and researchers who have access to medical files and other data.

Neumann discussed the identity work that his colleagues Brent Waters at SRI and Carl Gunter at the University of Illinois are undertaking in the area of attribute-based encryption, where access to a database is determined not by identity or title but by an explicit attribute that might be related to a role or characteristic. Carl Gunter’s attribute-based messaging system, for example, enables one to send e-mails to a select group of physicians, such as all surgeons who perform brain surgery, or all pediatric brain surgeons, or even to just those surgeons who excise brain tumors.

In the end, the inherent complexity of computer systems suggests there is no one-size-fits-all approach. “Instead,” says Neumann, “we must focus on building identity management systems that have well defined, enforceable policies and are considered trustworthy in the holistic sense of the systems and enterprises in which they exist.”

I3P researchers who delivered papers at the NIST symposium include Deb Bodeau of the MITRE Corporation, who presented an identity framework to facilitate information trustworthiness within a large organization; Jingwei Huang of the University of Illinois, who talked about ways to quantify the risk associated with trust in a public key infrastructure; and Ning Shang of Purdue University, who described privacy-preserving strategies for mobile devices.

The I3P will participate in this upcoming symposium on June 16th, 2009.
I3P Researchers Fix Security Hole in Control Systems

In a control system environment, an authentication process that requires a user name and password could lead to disastrous delays during an emergency. At the same time, knowing who has access to critical networks and what actions they are performing is important, especially in a world of proliferating cyber threats. How does one reconcile these conflicting security needs?

I3P researchers at Pacific Northwest National Laboratory (PNNL) have developed a solution in the form of an authentication tool that monitors network traffic and triggers alerts on specific control commands. The Non-obtrusive Authentication of Critical Infrastructure Operators (NACIO) tool identifies and verifies control system operators who issue critical commands without impairing access in an emergency. "Working with industry and following their recommendations," says team technical lead Samuel Clements, "we developed NACIO as a strictly passive system, one that does not impede network traffic."

NACIO follows a three-step process: First, when a predefined command is entered into the network, a photograph is taken of the operator at that workstation; second, a query is sent to an authentication device for credentials (e.g., badge, facial recognition, or token); third, the response from the authentication device is checked against a role-based access system and the result is logged.

Because NACIO creates an audit trail, with critical commands matched to the operators who issued them, along with details of actions taken, "the device is an important forensics tool," says Clements.

NACIO is one of several tools developed by the I3P to address security weaknesses in control centers. "Our intent," says Charles Palmer, Research Director for the I3P, "is to fill the security gaps identified by stakeholders as critical for control system operations. NACIO represents the missing link in the audit chain."

The NACIO team has filed a patent application for the tool and is currently seeking an industry partner to help make the technology commercially available. For more on NACIO and the I3P PCS project, visit the I3P website at http://www.thei3p.org.

Experts Gather for Insider Threat Workshop in Washington

The I3P Workshop on Insider Threats: Strategies for Staying Secure, held May 4-5 in Washington, DC, brought together representatives from academia, government and private industry to discuss the issue of insider threat from many perspectives, including legal, ethical, behavioral and technical.

On May 4th, workshop participants attended an open-to-the-public I3P poster session and a RAND Corporation congressional panel session on human behavior and cyber security, held in the Rayburn and Longworth House Office Buildings, respectively.

On May 5th, the invitation-only all day workshop showcased work accomplished by the I3P Insider Threat research team, whose members include Columbia University, Cornell University, Dartmouth College, Indiana University, MITRE Corporation, Purdue University, and the RAND Corporation.

The workshop addressed concerns ranging from employees masquerading as someone else to gain access to protected information and malicious insiders attempting to harm corporate networks or steal information to well-meaning insiders who cause damage inadvertently, or perhaps unknowingly empower a malicious outsider. The team's two years of research solicited experiences and input from practitioners, researchers and policy-makers, to ensure relevant and useful work that produced strategies for protecting and defending organizations' computer systems from unwelcome insider actions.

Jean Camp Named IEEE Congressional Fellow

Jean Camp, professor of informatics at the University of Indiana and an I3P researcher, has been named the IEEE's Congressional Fellow for 2009-2010. She will spend the academic year in Washington, DC, supported by the Congressional Science and Engineering Fellows program at the American Association for the Advancement of Science. This prestigious fellowship strengthens the relationship between scientists and policymakers, helping scientists understand the intricacies of federal policymaking while helping decision-makers understand the increasingly complex scientific and technical issues that underlie public policy.
Upcoming Events

June 16, 2009
Symantec Government Symposium
Ronald Reagan Building, Washington, DC
http://www.okco.com/symantecsymposium/200932

June 24-25, 2009
Workshop on the Economics of Information Security (WEIS)
University College, London, England
http://weis09.infosecon.net/

July 14, 2009
CISO Workshop
Tuck School of Business at Dartmouth College, Hanover, NH

For more information, contact laurie.burnham@dartmouth.edu
or 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”