

Message from the Chair

Strengthening Cybersecurity in the U.S.

At a recent hearing held by the House Committee on Homeland Security, several Committee members, including Chairman Thompson and Ranking Member Langevin, expressed concern that our nation's cyber infrastructure needs strengthening in this era of growing global threats from cyber terrorists and others with the ability to do significant harm.



The Institute for Information Infrastructure Protection (I3P) agrees the threats to information security are real and considers the protection of our nation's digital assets an urgent national issue. As Chairman Thompson remarked at the hearing, "cybersecurity is... maybe the most complicated national security issue... [and] will be with us for decades to come."

Many of the questions raised at the hearing are currently being tackled by the I3P, an institute dedicated to strengthening the cyber infrastructure of the United States. We function as an impartial, national forum on cyber security, undertaking research, identifying key R&D topics and seeking solutions through the power of inter-institutional and multi-disciplinary research. Managed by Dartmouth College, the I3P is an independent consortium with 27 members across the nation.

Our consortium brings depth and breadth to the field of cyber security and is engaged in a broad range of cyber security activities, ranging from research and development to hands-on workshops to technology transfer. Our four major research initiatives—on insider threat, identity management, process control systems, and the economics of cyber security—touch on many of the issues raised during the hearing: network monitoring, intrusion detection, resilience, information systems, legal framework and control systems disruption.

Moreover, we are currently meeting many of the needs identified during the hearing: we apply metrics to measure the impact of our work; we actively engage with industry to ensure our solutions meet real-world needs and we are developing a suite of software tools aimed at hardening security in critical areas, notably the oil and gas sector.

Although our work does not touch directly on the internal systems of the federal government, we are fulfilling our mandate to protect the cyber infrastructure—public and private—of the U.S. The I3P continues to bring our nation's best resources to bear on this complicated issue and will continue to work to move the U.S. toward a more secure future in cyber space. I invite you to call on the I3P at any time.

Charles C. Palmer
Chair and Research Director of the I3P

I3P Launches Scholar Program

In line with the I3P's role as a leader in cyber security, a Scholar Program has been established that will fund recent college graduates for one year of research at a consortium member institution.

Three scholars will be awarded a salary, plus travel and institutional costs, for a 12-month term of hands-on information security experience.

In addition to providing the scholars with an exceptional educational opportunity, the program will enhance the research of member institutions and add to the burgeoning national cadre of IT security researchers. Since 2003, the I3P has offered a Post-Doctoral Fellowship Program exclusively for PhD holders. In contrast, the new Scholar Program is intended for recent baccalaureate degree recipients and therefore, "targets the newest professional members in the field...to help build a national base of researchers and experts," said Heather Drinan, I3P Information Manager.

Both programs respond to a recognized need for greater expertise in the field, articulated in the 2005 President's Information Technology Advisory Committee (PITAC) report that described the American

The Institute for Information Infrastructure Protection (I3P)

Research Fellowships

for post-doctoral researchers, junior faculty and research scientists

Call for Proposals

APPLICATION DEADLINES
Applicants must submit proposals to the host institutions by February 8, 2008.
Host institutions must submit application packets to the I3P by February 22, 2008.

Program Description
The Institute for Information Infrastructure Protection (I3P) seeks to advance its national research agenda through a research fellowship program. The I3P fellowship program helps to build a nationwide cadre of investigators focused on critical research challenges and provides

IT infrastructure as "highly vulnerable to premeditated attacks with potentially catastrophic effects."

The report also declared that, "there simply aren't enough cybersecurity researchers, and no good mechanism for producing them."

The Scholar Program will serve as an important catalyst for a new generation of cybersecurity researchers.

Candidates will be selected based on academic qualifications, relevance of the program to the individual's long-term goals, and faculty recommendations. Applications are due April 4, 2008 and more information can be found at <http://www.thei3p.org>.

--Bridget Alex



Cyber disruptions, especially to process control systems, represent a real and growing threat to the United States. Control systems not only play a key role in the automation of industrial facilities, but they are increasingly connected via business networks to the Internet, which renders them vulnerable to external threats. Even a small process disruption by a malicious hacker could have serious safety, environmental and economic consequences.

Recognizing the need to harden this critical infrastructure, the I3P is hosting a hands-on security workshop in Houston on March 6 for the oil and gas sector. In the audience will be asset owners, control systems engineers, operators, security officers and vendors from the energy community. "Coming together in this format," says Robert K. Cunningham, team leader for the PCS project, "enables I3P researchers to work closely with industry to develop broadly applicable solutions."

The I3P develops tools, technologies and methodologies to harden control-system environments, and works with companies on best practices. As part of this process, asset owners and vendors have the opportunity to provide feedback and technical guidance, and thus directly influence the development of these tools. The upcoming workshop is the fourth such workshop hosted by the I3P.

I3P Hosts Workshop to Address Survivability and Recovery of Process Control Systems

--Bridget Alex

Bishop led the Red Team that engaged in open-ended, hands-on efforts to identify any means of vote-manipulation, including malicious acts by insiders and outsiders, as well as accidental voter errors.

"I honestly didn't know if there would be serious problems—I knew there were in the past...but I assumed they had fixed the problems and all would come out well. Unfortunately, I was disappointed," Bishop said.

The UC Davis researchers found that all three systems possessed fundamental security flaws that could have been avoided with the kind of basic safeguards taught in undergraduate computer science classes. Among other faults, the systems were susceptible to viruses that could flip and delete votes, scramble tabulation data, and spread between machines.

In response to the Red Team's report, Secretary of State Brown withdrew the systems and agreed to recertification provided that vendors and jurisdictions observe precautionary measures. Bishop said that Brown's actions were appropriate and that "she heard the message of the review."

Bishop hopes that other states will take notice. The study, he says, was instrumental to "protecting the integrity of California's elections, and we hope will help other states as they review their election equipment and procedures."

Mathew A. Bishop, professor of computer science at the University of California, Davis and a member of the I3P Executive Committee

Bishop's team was able to directly compromise the systems. In the most disconcerting approach, researchers broke the physical locks on voting machines and uploaded code that altered vote totals—an attack that took only a couple of minutes, or the amount of time an average voter spends at a machine.

Begun in March 2007, the study was commissioned by California's Secretary of State, Debra Brown as a part of the "Top-to-Bottom Review" of voting procedures, designed to restore public confidence in the electoral process. Three voting systems—Diebold, Hart, and Sequoia—were assessed on their security, accuracy, reliability, and accessibility.



The idea of voting elicits multiple emotions for Americans. To some, voting is a right; to others, a duty; to still others, a waste of time. Regardless of individual sentiments, fair and democratic elections are a tenet of Americanism and even those who eschew the polls are disturbed by the thought of votes being manipulated.

Yet this unsettling scenario was proven feasible by a team led by Mathew Bishop, an I3P researcher and professor at the University of California, Davis. The investigators tested three electronic voting systems used in California and found all three systems to be non-secure.

I3P Researcher Finds Flaws in Electronic Voting

Upcoming Events

The 4th Annual I3P PCS Security Workshop
March 6, 2008-Houston, TX

IFIP International Conference on Critical Infrastructure Protection
March 16-19, 2008-Arlington, VA

I3P Workshop on Insider Threats in the Networked World
April 15-16, 2008-Durham, NC

I3P co-sponsors workshop on economics of information security
June 15-27, 2008-Hanover, NH

For more information, please see the I3P calendar at <http://www.thei3p.org>