A Message from the I3P’s Research Director

One of the pleasures of being I3P Research Director is engaging with our member institutions. In that role, on October 29, I was delighted to be a judge in one of NYU-Poly’s activities for Cyber Security Awareness Week (CSAW): the AT&T Award for Best Applied Cyber Security Research Paper. The competition evaluated student papers that were submitted to or accepted at any conference or journal between September 1, 2009 and August 31, 2010. To be considered for the award, the papers had to pass an initial screening based on four criteria: originality, relevance, correctness and presentation, and to cover a topic related to applied security technology, systems implementation, or lessons learned. Of the ten finalists who presented their posters to the judges, three were declared winners:

2. Xin Hu (University of Michigan), “Large-Scale Malware Indexing Using Function-Call Graphs”
3. Abhinav Srivastava (Georgia Institute of Technology), “Automatic Discovery of Parasitic Malware”

This competition was one of several NYU-Poly CSAW activities, each of which was meant to encourage students to hone their cyber security skills: a capture-the-flag exercise, a high school cyber forensics competition, an embedded systems challenge, a cyber security trivia quiz, and a security awareness video challenge. (See http://www.poly.edu/csaw for more information and to view some great winning videos!)

Events such as the AT&T Research Paper Competition can encourage good students to stay in the pipeline and was a wonderful judging experience. But more of us need to be doing more to meet our nation’s need for cyber expertise. For this reason, the I3P hopes to play a significant role in addressing current workforce needs in cyber security. As a first step we will host a workforce development workshop at Georgia Tech in April 2011 to examine the demand for cyber expertise, a workforce issue that is often looked by organizations whose primary focus is on the supply side. We hope you will join us; please watch this space for more information.

--Shari Lawrence Pfleeger, I3P Research Director

I3P’s Charles Palmer Delivers Lecture at the MITRE Corporation

"Rethinking Cybersecurity: How many people does it take to secure the infrastructure?" was the title of a talk delivered by Charles Palmer, Senior Technical Advisor to the I3P, on October 14th at the MITRE Corporation.

Addressing the role individuals play in securing the IT infrastructure, Palmer described several scenarios where privacy and security matter to the user, mentioning that banking, shopping and anonymous postings on the Internet all trigger security and privacy concerns. Yet these concerns are fickle: under the right circumstances—such as when creating a social network profile or signing up for membership at a grocery store—individuals willingly give up their personal privacy. “We all want security,” Palmer said, “and we all want privacy to happen when we want it to happen.”

I3P Institutions join NEBULA Project to Work on Cloud Security

The National Science Foundation (NSF) recently awarded $7.5 million to fund the development of a ground-up security architecture for cloud computing. I3P member institutions Cornell University, Purdue University, the University of Illinois and the University of California, Berkeley, have joined five other institutions in a three-year effort to create NEBULA, a trustworthy cloud-computing network.

The goal of cloud computing is to send computing tasks (or data for storage) from a client to a centralized processing center, a strategy that boosts efficiency by cutting down on unnecessary computer capacity and programming time. But the underlying architecture that makes such efficiency possible has serious security limitations that the NEBULA researchers hope to overcome. If successful in developing a trusted cloud computing network, they envision a range of new applications relating to smart grid operations, financial transactions and especially medical care.

NEBULA’s architecture offers more than just security. The data centers that comprise the cloud could have significant environ...
At the same time, users have only so much control over the process. “Systems are smarter and more interconnected and there is more stuff online than ever before. Is that a good thing?” Palmer asked. When designing systems, programmers focus more on speed and functionality than on usability and security, he explained. People and their online behaviors are generally not factored into the design process.

It’s time for a sea change, he reflected. Programmers need to build systems from the ground up, harmonizing security with the user experience. “It’s not one problem area we should be concerned about; it’s all of them,” he said, stressing the need for a multidisciplinary approach when building new systems.

Palmer also talked of the need to educate the next generation of cybersecurity experts and to leverage more effectively the skills and knowledge of the people already in the workforce. “The number of geeks is shrinking,” Palmer warned, “at a time when the need for cyber experts is growing.” Not only do students at universities, colleges and community colleges need to be groomed, but also multidisciplinary experts, including anthropologists, lawyers and social scientists, must be brought into the fold.

At the same time, keeping ahead of determined and diverse cyber criminals remains a challenge. Some want to steal personal identities; others may want to bring down critical infrastructure. Our adversaries may be industrial spies, members of organized crime rings, rogue nation states or political dissidents, and they are already in the networks causing damage. Moreover, says Palmer, their goal isn’t necessarily to figure out and quietly penetrate a network, but to plan for something damaging down the road. “These guys need the Internet too,” Palmer said, “but they only need it once.”

Still, Palmer believes it is possible to build a secure system. The key, he says, is integrating people into the process. He recommends that the public have access to security tutorials, government officials receive regular briefings and students at all levels be taught basic concepts in cybersecurity. The human element must be considered upfront, if we hope to secure our networks; technology, he stressed, can only go so far. [To watch Palmer’s presentation, please visit http://www.thei3p.org/media/video/]

NIBULA
...continued from page 1

mental benefits. Electric power is greatly diminished when sent over long lines; according to Ken Birman, computer scientist at Cornell, as much as 80 percent of the Nation’s electricity is lost over these long lines. If NIBULA’s architecture can identify and prioritize the use of data centers located near power sources, electricity use will be cut significantly, thus reducing overall demand.

The environmental benefits of NIBULA do not stop there. Because computing power is moved from individual computers to shared data centers, idle times can be nearly eliminated, resulting in improved efficiency. “Cloud computing data centers [have the ability to] shift work around to minimize the power expenditures associated with solving problems,” says Cornell computer scientist Hakim Weatherspoon.

NIBULA is headed by Jonathan Smith of Pennsylvania State (not an I3P member); the project is part of a larger NSF initiative called the Future Internet Architecture that involves 60 researchers at more than 30 institutions. [For more information please visit: http://www.cornelluniv.com/section/news/content/2010/09/01/cornell-researchers-work-towards-safer-internet]
I3P Awards 2010-2011 Postdoctoral Fellowships

Two California researchers—one at SRI International; the other with a joint affiliation at Lawrence Berkeley National Laboratory and the University of California, Davis—have won I3P Postdoctoral Fellowships for the 2010-2011 academic year.

Minyoung Kim, a recent graduate of the University of California, Irvine, will spend this academic year with Ashish Gehani at SRI International, where she will examine security across multi-layered systems. She will focus specifically on ways to efficiently integrate security into the multiple components of a computing system (the operating system, applications, network stacks, hardware, etc.). By studying how these components interact and by adjusting their security policies, Kim hopes to strike a balance among such competing needs as security, service, energy efficiency, and system resource availability. The latter she says is especially important to industry professionals who make security decisions. “[Kim’s] focus on cross-layer optimization of security systems meets an important real-world need,” says Gehani, “and I think she will accomplish much this year.”

Sean Whalen, who recently earned his PhD at the University of California, Davis, will spend the academic year commuting between Lawrence Berkeley National Laboratory and UC Davis, expanding his research in metric-based anomaly detection with the guidance of Sean Peisert, who has appointments at both institutions.

Whalen hopes to develop new metrics by which to recognize and examine multiple cyber events on a network, work that will be applicable to both process control systems and supercomputing clusters. Moving from an ad hoc intrusion detection system to a more mathematical approach, Whalen’s design will allow a system to adapt to new attacks without raising a prohibitive number of alerts. If a system raises too many alerts, it can disrupt business operations and create an environment in which operators learn to ignore warnings, much like the “boy who cried wolf” scenario. “It will be a very interesting year with Sean,” says Peisert. “Not only does his work span both the practical and the conceptual, but he is everything one would want in a postdoc: innovative, entrepreneurial, open-minded, inquisitive and dedicated.”

Now in its seventh year, the I3P Fellowship program places recent PhD recipients at an I3P member institution of their choosing. “Having so many exceptional research institutions participating in the program appeals to our applicants,” says Ron Dodge of United States Military Academy and Chair of the I3P Fellowship Committee. Fellows become part of the larger I3P community and also have the opportunity to interact with top cybersecurity researchers through various consortium activities, such as meetings and workshops. For more information on the program, visit: http://www.thei3p.org/education/fellowships.html.

I3P Researchers in the News

Columbia’s Steve Bellovin speaks out against the FBI’s request that encrypted communications systems have backdoors for surveillance. “It’s a disaster waiting to happen,” says Bellovin.

- New York Times

Georgia Tech’s Mustaque Ahamed explains why botnets are hard to spot using home anti-virus software. “Bots are one of the most serious threats we face today,” says Ahamed.

- The New York Times

Alessandro Acquisti of Carnegie Mellon reflects on the shifting values of privacy, noting that formerly questionable online behavior is now increasingly the norm.

- American Public Media

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

March 23–25, 2011
IFIP International Conference on Critical Infrastructure Protection
Dartmouth College in Hanover, NH
http://www.ifip1110.org/conferences/

April 5–6, 2011
The First Software and Usable Security Aligned for Good Engineering (SAUSAGE) Workshop
National Institute of Standards and Technology, Gaithersburg, MD

April 27–28, 2011
Workforce Development Workshop
Georgia Tech in Atlanta, GA

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”