A Message from the I3P's Senior Technical Advisor

One year ago Carl Landwehr of IARPA and the National Science Foundation asked the I3P to coordinate a workshop on how to best design a secure system engineering competition. The idea has historical precedent: competitions have been used for centuries to spur innovation. In the area of computer security, competitions have been held in such areas as hacking, programming and algorithm design. Yet, with the exception of the Advanced Encryption Standard competition and despite their popularity, computer security competitions have made few lasting contributions to security. If a competition-based approach is believed to be a good path toward innovation, then another kind of competition needs to be found.

Our workshop, which took place in April, drew together an extraordinary group of people dedicated to the challenge at hand, namely: if one were to hold a competition to solicit ideas for ways to make computer systems far more secure than they are today, how might such a competition be designed and what would its criteria for success be?

More than 50 participants distributed themselves among three discussion topics: foundational security components (system-level components that would enable more secure systems), secure system implementation (tools and components that would enable others to build more secure systems), and workforce development (reversing the current shortfall). After three days of idea sharing and brainstorming, several intriguing competition themes were proposed, including building a secure development tool chain, implementing a secure voting system, and a recurring competition called the Cyber Cup (think Americas Cup).

We are now wrapping up a summary report for the workshop and plan to release the results publicly. Then we'll be working with interested groups to further refine the definitions and rules of the most promising competitions. We'll go for the grand prize by presenting the best competition plans to potential sponsors. Good luck to all the competitors!

--Charles Palmer, Senior Technical Advisor to the I3P
Clifford Grant, of Pacific Northwest National Laboratory, introduced NACIO (Non-intrusive Authentication of Critical Infrastructure Operators), a forensic tool that not only detects and tracks critical control-room commands but also ties them to a specific operator. Should a malicious event occur, the person who entered inappropriate code can be identified and held accountable.

Michael McDonald, of Sandia National Laboratories, then spoke about an operator simulation tool called OPSIM. Control-room employees who participate in simulation exercises, he explained, have a better grasp of how intelligent adversaries design and execute attacks, and, more important, are better equipped to recognize and respond to attacks in real time.

Finally, Gordon Rueff, of Idaho National Laboratory, introduced the crowd to a conceptual tool called PHIA, which was developed with funding from DOE’s National SCADA test bed. A network management tool, PHIA reduces the need for human surveillance in the control room and thus can be a cost-effective option for utilities worried about inappropriate activity on their control network.

Drawing the session to a close, Palmer reflected that, “control systems, which represent the nexus between the cyber world and the physical one, are where the rubber hits the road. We know they’re being penetrated, we know we have to protect them and we know that we have to protect them on multiple fronts. Although the challenges are many,” he added, “we are fortunate today to have heard about a suite of tools being developed that could have a significant impact on security.”

If the speed with which information sheets flew off the table at the back of the room is any indication, interest in the presentations and the I3P tools suite was high.

Privacy Holes

In SSN assignment. Once they identified specific patterns, they interpolated the data using a live person’s date and place of birth to predict the range and values of individual SSNs. The data set thus narrowed, they could identify individual SSNs utilizing statistical analysis and brute-force matching, a process as easy as cracking a 3-digit PIN.

The problem, according to Acquisti, is that SSNs are inappropriate identifiers and should be phased out in favor of a new system. “There needs to be a distinction between identifiers and authenticators,” he said. “For example, your phone number is an identifier; people can reach you by calling your number. Your SSN acts in a similar manner, with the number and name co-linked. By contrast, the passcode to check your voice messages, just to give one example, is an authenticator; the only person who knows it is you.” Currently, SSNs act as both identifiers and authenticators.

The ubiquity of online personal data on sites like Facebook, Myspace, Amazon, and even Netflix, has many experts worried about how much information can be collectively gleaned about an individual. Last year students at MIT found they could determine—with 78 percent accuracy—a person’s sexual orientation simply by analyzing their friends’ Facebook pages.

Acquisti encourages individuals to assume everything they do online is public, and to protect their sensitive data with currently available technology, such as encryption and anti-virus software. But he also recognizes the difficulty in convincing the public to take these steps. Technological know-how and awareness are factors, but so is the rising nonchalance over privacy. “Online privacy is slowly being eroded, and the consequences are not always immediately perceivable. This disconnect makes it easy for the public to brush off the consequences.”

For more information on Acquisti’s SSN study visit, http://www.heinz.cmu.edu/~acquisti/ssnstudy/
I3P Sponsors 4th Annual IFIP Conference

The I3P sponsored the fourth annual gathering of an international working group of researchers at the National Defense University, Fort McNair, Washington, D.C., on March 14 - 17. The Fourth Annual IFIP Working Group 11.10 International Conference on Critical Infrastructure Protection included 54 participants from 11 countries. This working group is part of IFIP, the non-governmental, non-profit International Federation for Information Processing. IFIP functions as an umbrella organization for more than 100 Working Groups in various fields of information processing, made up of over half a million individuals from 56 countries.

The principal aim of IFIP Working Group 11.10, as described on its website, is to “weave science, technology and policy in developing and implementing sophisticated, yet practical, solutions that will help secure information, computer and network assets in the various critical infrastructure sectors.”

The working group met over the three days to discuss topics in the areas of Control Systems Security, Infrastructure Security, Risk Analysis and Management, Intrusion and Anomaly Detection, Tools and Techniques, Interdependency Modeling and Propagation, and Security Assessment. Examples of specific topics within these areas are as diverse as “Modeling Control System Failures and Attacks – The Waterloo Campaign to Oil Pipeline,” presented by Jonathan Burts of the University of Tulsa, to “U.S. Federal Regulatory Oversight of Rail Transportation of Toxic Inhalation Material,” presented by Rajni Goel of Howard University and “Protecting the Food Supply Chain from Criminal Manipulation and Terrorist Attack” by Roberto Setola of the University of Navarra.

Highlights of the conference were the three keynote talks, the first given by Lieutenant General Keith Alexander, Director of the National Security Agency. Mischel Kwon, Vice President, Public Sector Security Solutions at RSA and former Director, U.S. CERT, spoke on “Cyber Security, Crime, Espionage, War or Silo… The Critical Infrastructure Reality,” and Alan Paller, Director of Research for the SANS Institute discussed “A Tale of Two Departments – How the Departments of State and Commerce Responded to the Same Nation-State Cyber Attack.”

Selected presentations from the conference may be viewed at thei3p.org/events/ifip2010.html. The conference proceedings will be published next summer by Springer as Critical Infrastructure Protection III, and the next meeting of the IFIP Working Group 11.10 will take place at Dartmouth College in Hanover, NH, March 23-25, 2011.

For the latest news and updates on I3P research, visit the I3P website at www.thei3p.org.

I3P Researchers in the News

Kevin Fu of UMass, Amherst, speaks to CNN about the perils of pacemakers and other wireless devices.

Georgia Tech researchers, including Mustaqe Ahamad, share their expertise with the Telecommunications Industry Association (TIA) Standards Committee.

The GhostNet botnet—discovered last year by a research team that includes Shishir Nagaraja of the University of Illinois—is now blamed for stealing missile data from India.

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

July 22–23, 2010  
Cybersecurity through a Behavior Lens  
National Capitol Visitor Center in Washington, DC

November 16–17, 2010  
Systems-based Cybersecurity  
University of Virginia in Charlottesville, VA

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

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”