



# Institute for Information Infrastructure Protection

Newsletter Volume 1, Issue 2

June 2008

## Message from the Executive Director

In its sixth year, the I3P has made—and continues to make—important contributions to the field of cyber security. Our five research projects in such critical areas as process control systems security, identity management and risk pricing have produced results ranging from peer-reviewed publications to commercialized software. We are, of course, proud of this research.

But devising solutions and meeting existing needs is not all we do. Our mission also impels us to look ahead: to identify and address emerging issues before they become noted problems. To this end, we fund preliminary studies on an array of topics, producing white papers that have the potential to become major new avenues of research. Two such papers, one on medical telemetry; the other on attribution, are described in this newsletter.

At the same time, we continue to actively engage our many stakeholders in constructive dialogue, working hard to stay ahead of the curve in a world of ever changing cyber threats. As the current Administration winds down and the nation prepares for a new President, the I3P will continue doing what it does best – collaborating with academia, industry and government to identify and find solutions for cyber security problems.

--Martha Austin, Executive Director



availability (the devices must perform accurately when needed); integrity (they must transmit only valid data); and authentication (the data must be linked to an identified source.)

“History,” says Fu, “has taught us that it is more important to build security into a system during the beginning stages, as it is more difficult to add security later.” *Protecting Global Medical Telemetry* can be read in its entirety at: <http://www.thei3p.org/research/whitepapers.html>.

--Kiel Alarcón, I3P Communications Assistant

## Economics Workshop Coming to Dartmouth

Later this month, from June 25 to June 28, the seventh Workshop on the Economics of Information Security (WEIS) will be held at Dartmouth College in Hanover, New Hampshire. The conference, hosted by Dartmouth’s Tuck School of Business and Institute for Information Infrastructure Protection (I3P), will draw about 100 participants hailing from at least ten different countries.

A diversity of experts, including academic technologists, social scientists, legal scholars and business executives, will convene on campus to address how economic, behavioral, and legal factors affect the security and dependability of information and information systems.

Eric Goetz, associate director for research at I3P and an organizer of the event, says WEIS provides a unique venue for assessing cyber-security decision-making in a business context. Unlike investing in marketing, the impact of which can be measured in sales and revenues, cyber security lacks markers for success.

“There’s no monetary or measurable payback on that investment,” Goetz explained. “Events like WEIS provide an opportunity to look outside the box and discuss new models for linking business value to cyber security.”

Companies represented at WEIS include Microsoft, HP Labs, Merrill Lynch, Goldman Sachs, CVS Caremark, and Sprint, and academics attending the workshop hail from all over the world.

More information about the conference can be found at <http://weis2008.econinfosec.org>.

--by Jennifer Garfinkel, Dartmouth class of '08

## Medical Devices: An Emerging Security Threat?

In a provocative white paper, I3P researcher Kevin Fu and colleagues at the University of Massachusetts, Amherst, describe a new medical telemetry infrastructure created by proliferating implantable medical devices (IMDs).

These devices can be lifesaving, as in a pacemaker that delivers a sudden shock to a failing heart, as well as liberating for patients, who can cut back on doctor visits and exert better control over their pain.

Many IMDs, which also include heart-rate sensors, drug delivery systems and nerve stimulators, operate wirelessly. Therein lies the problem: like other wireless technologies they may become vulnerable to future cyber threats.

The solution, according to Fu and his colleagues, is to design wireless medical devices with four security goals in mind: privacy (thus ensuring protection of personal information);



Kevin Fu (top left) working with colleagues on IMDs



M. Eric Johnson of the Tuck School of Business engages with attendees at a previous information security workshop

## I3P Researcher Addresses Attribution

One of the principle foundations and arguably greatest strength of the Internet is the forum it provides for the free exchange of ideas. Such freedom is made possible partly by the ability to remain anonymous, an often important companion to free speech. While many of us champion this ability, there are inherent problems with the free-speech model when applied to the Internet. Cyber criminals, for example, can conduct attacks anonymously, making their identification and prosecution almost impossible.

Two I3P researchers, Jeffrey C. Hunker of Carnegie Mellon University and Robert Hutchinson of Sandia National Laboratories, along with Jonathan Margulies, explore the issue of attribution in a white paper that also addresses the risks associated with Internet anonymity.

"The subject has interested me for some time," says Hunker, "in part because so little attention has been paid to the issue. It was Hutchinson's suggestion that we apply our combined technical and policy perspectives to the problem. He was entirely right."

While the Internet must retain enough anonymity to ensure the free exchange of ideas (e.g., by facilitating discourse in countries with repressive regimes), enough attribution is needed to suppress and, if necessary, respond to cyber attacks. "Our legal and policy frameworks for responding to cyber attacks cannot work unless we have adequate attribution," the paper reads.

Yet the Internet community largely resists attribution, seeing value in anonymity. At the same time, important logistical and technical questions remain unanswered. Among them is the issue of work-arounds, that is, circumventing the system by creating an anonymous subnetwork that makes it impossible to determine the source of the original message.

Incentives, say the paper's authors, must be found that will convince users as well as service providers that attribution models are both necessary and prudent. Such incentives can include, but are not limited to, the need to combat growing cyber crime and, adds Hunker, "the prospect that we will at some point see visible signs of cyber terrorism."

Overall, the issue of attribution is likely to grow in importance over the next several years and may need to be resolved with the help of a multinational framework. To read *Roles and Challenges for Sufficient Cyber-Attack Attribution*, visit the I3P White Paper page at <http://www.thei3p.org/research/whitepapers.html>.

--Kiel Alarcón, I3P Communications Assistant

## Dartmouth Student Examines Internet Governance

The Internet has emerged as an indispensable global medium, facilitating commerce, opening channels of communication and leveling the playing field of knowledge around the world. Yet its long-term stability and security are far from



**Jeffrey Hunker believes the prospect of cyber terrorism increases our need for proper attribution.**

certain, as exemplified by the controversy over its governance.

The issue of governance is being explored in depth by Elma Demir, a graduate student in globalization studies at Dartmouth College. Supported by the Institute for Information Infrastructure Protection (I3P), Demir has spent the past six months researching the security implications of a proposed shift in governance from the unilateral one that currently exists to a multilateral one.

Since 1998, a U.S.-based, non-profit organization—the Internet Corporation for Assigned Names and Numbers (ICANN)—has controlled administration and management of the Internet. Operating with oversight from the U.S. government, ICANN coordinates (among other things) the allocation and assignment of domain names, protocol addresses and server systems.

This Internet governance arrangement is now being questioned, with some nations asking for internationalization of the Internet so that no one nation has sole control over the medium. The U.S., however, hopes ICANN will retain control over the Internet, claiming that a more multilateral system could jeopardize the security and stability of the global information infrastructure. This claim forms the crux of Demir's analysis.

Originally from Bosnia-Herzegovina, Demir is finishing her third semester as a Dartmouth graduate student. Before landing in Hanover, she attended college at the University of Sarajevo and worked in her home country conducting public policy research. Demir chose Dartmouth for her graduate studies – the only school to which she applied – because it allowed her to design her own curriculum through the Master of Arts in Liberal Studies program.

In Demir's paper, which she intends to publish soon, she concludes that a switch to multilateral control would enhance Internet security—if necessary precautions are taken—and argues in fact that the Internet may be endangered if international agreement on Internet oversight is not reached.

"Unfortunately, the reality is that extremists and opponents of the United States are more likely to attack the Internet if they see it as a U.S. strategic asset," she explains. In addition, she says other countries may rebel by developing their own networks, an action that could further jeopardize security and fragment the Internet.

In the winter of 2009, after her next and last semester at Dartmouth, Demir plans to work as a research analyst in her home country before going back to school for a Ph.D. in political science.

--Jennifer Garfinkel, Dartmouth class of '08



**The Internet's long-term well-being calls for multilateral governance, says Dartmouth student Elma Demir.**

For more information contact Laurie Burnham, Editor at:  
laurie.burnham@dartmouth.edu

To subscribe or unsubscribe send an email to kiel.h.alarcon@dartmouth.edu with the subject line "Add/Remove I3P Newsletter Subscription"