Martin Wybourne, the Vice Provost for Research at Dartmouth, has named Denise Anthony, Associate Professor and chair of Sociology, the new Research Director of the Institute for Security, Technology, and Society (ISTS), formerly the Institute for Security Technology Studies. With this change in leadership, ISTS will continue its focus on cyber security and trust, but will broaden its scope to consider the role of information technology in society, particularly its impact on privacy and security broadly conceived.

“I very much look forward to working with Denise and the ISTS faculty as they address complex issues that require a combination of technical and social science expertise, such as privacy and trust,” said Wybourne. “I anticipate the broader scope of ISTS will attract new faculty and student interest to the many challenging questions presently facing information technology.”

Anthony, at Dartmouth since 1999, has been affiliated with ISTS since 2002. Her research focuses on how social dynamics affect communication, cooperation, and security in the use of information technology. As an adjunct assistant professor in the Department of Community and Family Medicine at Dartmouth Medical School, Anthony also will bring added expertise in the health care arena, where ISTS is engaged in several new projects considering the implications of information security in medical environments.

Inside This Issue

- Securing the eCampus Conference .................................................. 3
- Summer Robotics and Security Program .............................................. 3
- Business Essentials for the Information Security Professional .......... 4
- SISMAT ............................................................................................. 4
- Congratulations Graduates................................................................. 6

Continued on page 2
ISTS on the Road continued from page 1

At EuroPKI 2008 (June 16-17th, Trondheim, Finland), Pala presented results that extend PRQP in order to distribute pointers to PKI resources over a Peer-to-Peer (P2P) network. In particular, the research conducted by the UPKI/Trust Laboratory team, has introduced, for the first time in PKIs, the use of a Peer-to-Peer system based on Distributed Hash Tables (DHTs).

On June 11th, at the 3rd Annual TeraGrid Conference in Las Vegas, NV, Scott Rea jointly presented a paper with Dr. Margaret Murray from the Texas Advanced Computing Center, on using Levels of Assurance (LoA) as a catalyst for Identity Management across trust boundaries. As enterprise PKIs interact with other authentication communities such as those based on corporate directories (e.g. LDAP), or assertion based communities (e.g. shibboleth), the use of Secure Assertion Markup Language (SAML) can facilitate the passing of credentials with a different implied trust-ability or assurance to those issued by PKIs, between the differing communities.

The next day (June 12th), at the Seventeenth Federal Government - Higher Education (Fed/Ed) PKI Coordination Meeting in Washington, DC, Rea presented an overview of PKI projects operating within the higher education community, including the Higher Education Bridge Certificate Authority (HEBCA); the US Higher Education Root (USHER); and the IETF, as well as introduced PRQP to participants and invited feedback on the work being conducted by the UPKI project. Fed/Ed is hosted semi-annually by EDUCAUSE and provides an opportunity for US higher education institutions, PKI related vendors and researchers, and US government agency representatives, to discuss and coordinate PKI initiatives within their respective communities.

In June, Rea also helped to found the Four Bridge Forum (4BF) – a joint initiative between the current four US-based PKI bridges – HEBCA for US higher education, Federal Bridge CA (FBCA) for the federal government PKI, Signatures and Authentication For Everyone (SAFE) for the biopharmaceutical community, and the aerospace industry PKI bridge called CertiPath – to undertake outreach and education activities to promote the benefits of the use of bridge PKI technology. Several meetings have been held to focus the primary activities of the forum and define the agreement and specific action plan the forum will seek to implement.

Further challenges and research activities are still to be faced on the UPKI project, but the success of the research, development, and outreach initiatives of the project can be best demonstrated in the interest displayed in the results of the project to date. Many requests for information, invitations to speak at various conferences in global locations, and the actual deployment of the technology, is testimony to the importance of the work being carried out and its relevance on a truly global scale. Usability is a critical aspect of any security system, and in that regard, the UPKI project undertaken by ISTS researchers is helping PKIs world-wide become more usable, and more secure.

SCADA System Fuzzing and Wireless Fingerprinting

In August, Sergey Bratus presented the results of two efforts at the BlackHat conference in Las Vegas. BlackHat is the commercial counterpart of Defcon and takes place right before it. The conference offers both training and briefings for industry and government IT security personnel; security-related software and hardware vendors are also strongly represented.

The industry audience is why Bratus and his collaborators from industry, working together on the Trustworthy Cyber Infrastructure for the Power Grid (TCIP) project, chose to present the results of their SCADA system fuzzing project at BlackHat; understanding that people in charge of control networks would be attending, as well as vendor representatives. The goal was to inform the industry representatives of the study findings, capture their attention, and encourage them to check their own control network assets for similar weaknesses.

Unfortunately, the team could disclose very little of the actual technical details because of various concerns regarding the sensitivity of the research from a number of different parties involved. Their challenge was to give just enough detail to convince the practitioners that the threat was real. Judging by the reaction of several industry people present, it went well.

The other talk Bratus presented was on the results of the 802.11 wireless fingerprinting effort. Other members of the project team include: Cory Cornelius, Dan Peebles and Axel Hanson (see our last newsletter for more information on this project, funded by ISTS in 2007). Through the “fingerprinting project”, the team demonstrated a fast and inexpensive way of checking whether an open access point operates on the type of hardware that it claims to have. For example, if a laptop set up to attack users of the Dartmouth Public network would spoof its MAC address to appear as one of the legitimate Aruba access points, their method would reveal the deception.

New Mission continued from page 1

“I see my role as threefold,” said Anthony. “To build on the strong foundation of interdisciplinary work at ISTS by increasing connections to the social sciences and humanities; to increase awareness of ISTS within the Dartmouth community; and finally to advance the understanding of how IT security and privacy relates to socio-economic forces, cultural values, and political influences.”

Anthony takes over at ISTS following three years of leadership under Professor of Computer Science David Kotz. Regarding Anthony’s appointment Kotz said, “I am thrilled to have Denise leading ISTS. She brings a deep understanding of the nature of trust, a track record of interdisciplinary research, and an exciting vision for the future of ISTS.”

For more information, please visit the Institute’s redesigned website at www.ists.dartmouth.edu.
ISTS and PKCS to Host Second “Securing the eCampus” Conference

Long a leader in computing, Dartmouth College will host its second Securing the eCampus: Building a Culture of Security in an Academic Institution conference on November 11-12. Focusing on the unique challenges of cyber security in academia, the conference welcomes CIOs, CISOs, and other academic leaders to discuss and explore what it takes to develop a more secure information environment on college campuses.

Dartmouth has a history of computing that dates to a demonstration of remote computer access over telephone lines by Bell labs’ George Stibitz in 1940, through the creation of the BASIC computer language by former professors John Kemeny and Thomas Kurtz in the 1960s, to the present as one of the first campuses to offer ubiquitous wireless network access. This workshop focuses on security, a topic that has become so critical to every aspect of an institution’s operation, and it is co-sponsored by Dartmouth’s Institute for Security, Technology, and Society and Dartmouth’s Peter Kiewit Computing Services (PKCS).

Ellen Waite-Franzen, Vice President for Information Technology and Chief Information Officer at Dartmouth and a co-host of the event, notes: “When I started in this business, we all knew that computing technology was exciting, fast-moving, and sometimes risky. But the risks 10 years ago were nothing like the exposures we face today. Today, the lives of our institutions depend on network services at every single level, and it’s critical to constantly review security best practices and consult with our colleagues to maintain the computing trust of our constituents.”

Professor Denise Anthony, Research Director of the Institute for Security, Technology, and Society, chair of the Sociology Department, and the other co-host of the conference agrees adding, “Computing is a topic and a theme that intersects every academic and administrative department on a college campus. Recognizing computing as the collective resource that it is can help to ensure that we work cooperatively to address not only our individual needs, but also to share information and work together to address security and privacy issues that challenge us all.”

The 2008 program was developed considering comments from last year’s event. The first day of the conference will be held at the Courtyard by Marriott in nearby Lebanon, N.H., and will feature presentations from academic, industry, and journalist IT leaders who will present on a variety of topics including:

• Getting executive support for security programs
• Tensions between securing against legal pressure (i.e., copyright complaints, CALEA, etc.) and maintaining an open environment
• Developing an information security awareness program

Day two will be held on the Dartmouth campus and will feature several sessions including:

• Building a Security Operations Center
• Emerging trends regarding digital investigation and how they might impact incident response preparedness
• Authenticating remote learners
• Developing an information security course

For the detailed agenda, speaker bios, and registration information, please visit the conference website at: http://www.dartmouth.edu/comp/about/conferences/security/

The conference is receiving generous support from Cisco Systems and Presidio Networked Solutions.

Summer Robotics and Security Program

Once again this year, the Summer Robotics and Security Program offered an opportunity for high school students to learn about cyber security from an applied research perspective. This year’s “Make and Break Cryptographic Security Camp” focused on the understanding of mathematical principles used in cipher design and cryptanalysis, as well as designing and breaking cryptographic ciphers. There was no charge for this camp, which was sponsored by the Office of the Provost, the Department of Computer Science, and the Institute for Security, Technology, and Society.

Through a series of hands-on activities, high school students in 10-12th grades from four high schools were introduced to the concepts of symmetric and asymmetric cryptography. Activities included historic cryptanalysis of the Enigma cipher machine used in the Second World War; operating an electronic version of the Enigma; exploring modular arithmetic; designing the Diffie-Hellman key-exchange protocol; experimenting with RSA and some of the weaknesses of “textbook RSA”; and finally applying several code-breaking techniques in a grand challenge treasure hunt. Students also participated in a security reading group activity to encourage critical thinking about relevant topics by reading and discussing a paper on cryptography.

Continued on page 4
The week’s agenda included presentations and contributions by Christen Shepherd ’00, from the Department of Defense; Cory Cornelius ’07, ISTS researcher; a visit to the Hood Museum led by the Curator of Education, Lesley Wellman; Loren Thompson and Paul Pollack ’08, Department of Mathematics; Anne Perbohner, Dartmouth College sciences librarian; and Kevin Baron and Benjamin B. Homelson-Meister of the Thayer School of Engineering.

The topics and content were identified and developed over a period of many months by Dartmouth instructors Apu Kapadia (ISTS Post-Doctoral Research Fellow) and Patrick Tsang (Department of Computer Science doctoral candidate), and Suzanne Thompson (visiting scholar and director of the program), who developed and led this effort.

For additional information on the Summer Robotics and Security program see http://www.cs.dartmouth.edu/robot-camp or contact Suzanne Thompson, Program Director, at Suzanne. Thompson@Dartmouth.edu.

**SISMAT**

ISTS recently developed SISMAT (Secure Information Systems Mentoring and Training), a comprehensive program of education, training, and collaboration in information security. Through this program, Dartmouth and ISTS personnel led an educational outreach effort to help foster expertise in computer security at colleges within the northeastern United States. Over the summer term (the start of SISMAT’s pilot year), ISTS hosted seven undergraduates from different colleges as part of a comprehensive instructional, educational, and research program in information security.

Students were invited to campus for an intensive two-week lab and seminar training course in authentication, PKI, and methods of network attack and defense. Students were invited to attend the opening session of WEIS (Workshop on the Economics of Information Security, held at Dartmouth in June and hosted by the Center for Digital Strategies at the Tuck School of Business) and enjoyed talks from several invited speakers, including Doug Madory, the director of Dartmouth-Hitchcock Medical Center’s (DHMC) Information Security team; Christen Shepherd, a Department of Defense employee and Dartmouth alum; Scott Rea, a member of Dartmouth’s Peter Kiewit Computing Services (PKCS) and ISTS, and Dr. John Marchesini, a former PhD student of Professor Sean Smith of Dartmouth.

ISTS personnel also hosted the faculty mentors of the SISMAT participants for a weekend that focused on how to help transfer more information security concepts and techniques into the mainstream undergraduate curriculum. The weekend also showcased PKCS’s efforts related to their Cyber Security Initiative (CSI; for more information see http://www.dartmouth.edu/comp/support/library/safe-computing/initiatives/education/csi.html) as well as the work of two undergraduate Women in Science Project (WISP) participants. Feedback from the SISMAT participants and their mentors was universally positive.

After the course work, students spent the rest of their summers in internships that ISTS staff helped them find. Intensives were held at Ernst & Young, DHMC, the Federal PKI Policy Authority, Peter Kiewit Computing Services, General Dynamics, and the University of Michigan.

In the coming term, ISTS personnel plan to work closely with the students and their faculty mentors to undertake research projects at their home institutions. SISMAT aims to sustainably meet the goals of security education development by offering ongoing training and community-based resources to faculty members. ISTS researchers designed SISMAT to help construct these conduits of information from “real world” security practitioners to the academics who develop undergraduate security curricula.

**Business Essentials for the Information Security Professional**


BESP is designed specifically for heads of information security of Global 1000 companies and their direct reports. The program enhances fundamental business skills, so that executives can engage more effectively with other business leaders throughout their
enterprises. Participants also develop a more strategic mindset to help them communicate security risk to the organization and demonstrate information security’s core value to the business. Throughout the course, participants were given opportunities to network and leverage colleague strengths, as well as share best practices, providing insight to a variety of approaches to information security challenges faced across industries.

The four-day course was a joint offering of the Center for Digital Strategies and Tuck Executive Education. For information on attending the 2009 BESP program, contact Jennifer Childs (Jennifer.E.Childs@Dartmouth.edu), Program Manager.

**ISTS Affiliate Named to Technology Review’s Annual TR35 List**

By Susan Knapp, Dartmouth Office of Public Affairs

Tanzeem Choudhury, an assistant professor of computer science at Dartmouth College and a faculty affiliate of the Institute for Security, Technology, and Society (ISTS), has been named to the 2008 TR35, an annual listing from *Technology Review* magazine that features the world’s top innovators under the age of 35. Choudhury, originally from Bangladesh, is recognized for her research in developing computational techniques to better understand and predict human activities and social interactions.

“I use sensors to make sense of people,” says Choudhury, talking about using mobile sensors, tiny computers that can be embedded virtually anywhere, such as on a person, in cell phones, in a car or on a bicycle. “My research involves developing machine learning and sensing techniques to collect and analyze data about day-to-day human behavior.”

Choudhury, 33, who recently came to Dartmouth from a research position at Intel Research in Seattle, has developed techniques that can identify the most influential people in a social network by processing people’s patterns of speech in conversations. She believes that sensor-laden cell phones in the future will be able to identify behavioral patterns that are predictive of people’s health, productivity, and even social influence.

One of Choudhury’s current projects, sponsored by ISTS and funded by the National Institute of Standards and Technology (NIST), is titled “Discovery Trends in Activity-Aware Computing Environments.” This initiative involves developing algorithms that discover activity trends, derive quantitative metrics for finding people who are behaviorally alike, and identifying possible strategies to address some of the privacy concerns that this research uncovers.

“The TR35 honors young innovators for accomplishments that are poised to have a dramatic impact on the world as we know it,” said Jason Pontin, editor in chief and publisher of *Technology Review* magazine. “We celebrate their success and look forward to their continued advancement of Technology in their respective fields.”

Choudhury and the other TR35 winners for 2008 were featured in the September issue of *Technology Review* magazine and honored at the EmTech08 Conference held at MIT in Cambridge, Massachusetts. September 23-25, 2008.

“Being named to the TR35 list is well deserved for Tanzeem,” says Associate Dean of the Sciences C. Robertson McClung. “Her work has fascinating potential in this technological era of constant communications and relentless data gathering. I know our students will enjoy working with her. We are delighted to have recruited her to Dartmouth.”

**New ISTS Research Project:**

**Information Technology in Healthcare**

The Information Technology in Healthcare (ITH) project kicked off in June. The project is funded by the National Institute of Standards and Technology (NIST) and is being led by Professor Denise Anthony, in collaboration with Professor Eric Johnson and Post-Doctoral Fellow, Ajit Appari.

The project analyzes how hospital use of IT overall, as well as specific investment in IT security, is associated with the cost and quality of care. The research team will link two sources of hospital-level data and conduct multivariate statistical analyses to examine the relationship between hospital IT and spending and quality:

1) Data on the use of Healthcare IT systems in hospitals from the Dorenfest Institute for Health Information.


**A New Website**

As was noted in the lead story on ISTS’ new director and name and mission changes, we have redesigned our website. All of the information we previously provided is still available, including all past publications and project summaries. Please take some time to visit the new site and let us know what you think: http://www.ists.dartmouth.edu
Congratulations Graduates!

The following students have been involved with ISTS research and graduated in 2008:

Udayan Deshpande, Ph.D.
Title: “A Dynamically Refocusable Sampling Infrastructure for 802.11 Networks”

Shane Eisenman, Ph.D., Columbia University
Title: “People-Centric Mobile Sensing Networks”

Alexander Iliev, Ph.D.
Title: “Hardware-Assisted Secure Computation”

Ming Li, Ph.D.
Title: “Group-Aware Stream Filtering”

Chris Masone, Ph.D.
Title: “Attribute-Based, Usefully Secure Email”

Soumendra Nanda, Ph.D.
Title: "Mesh-Mon: A Monitoring and Management System for Wireless Mesh Networks”

Igor Paprotny, Ph.D.
Title: “Design, Fabrication and Parallel Control of Distributed Systems of Stress-engineered MEMS Microrobots for Microassembly”

Libo Song, Ph.D.
Title: “Evaluating Mobility Predictors in Wireless Networks for Improving Handoff and Opportunistic Routing”

Nicholas Willey, Master of Engineering Management

Jeff Fielding, A.B. Computer Science
Senior Theses Title: “Linkability in Activity Inference Data Sets”

Chetan Mehta, A.B. Economics

Fall Speakers

Dr. Greg Conti
United States Military Academy
Evil Interfaces: Violating the User
October 3rd

Dr. Andrew Martin
University of Oxford
Towards Trusted Grid Computing
October 17th

Dr. Marc Donner
Google
Security Pragmatics
October 23rd

Window Snyder
CSO of Mozilla
October 30th