From Our Director

E ducation is a recurrent theme in this issue of our newsletter. Cyber security and trust are ever more important challenges in our society, and to meet these challenges we need to educate the next generation of security professionals, raise awareness among the broader population, and within academia to improve our own security practices. ISTS has several initiatives underway. At right, you can read about our recent regional summit for CIOs of colleges and universities, discussing many of the challenges of “Securing the eCampus”. Inside, read about our week-long cyber security camp for local high school students, and about a new textbook on The Craft of System Security by ISTS affiliate Professor Sean Smith.

I’d also like to draw your attention to two exciting new initiatives coming next year. First, ISTS is sponsoring a 4-day program entitled “Business Essentials for the Information Security Professional,” to be held on May 12-16, 2008 at the Tuck School of Business at Dartmouth College. Many information security professionals find their security initiatives hindered because of their inability to communicate effectively within the enterprise (their organization/corporation). This program will help these senior security executives enhance their business skills and understanding so that they may engage more effectively with business leaders within their firms.

Second, ISTS is sponsoring a summer program for undergraduates in our region, “Secure Information Systems Mentoring and Training (SISMAT).” Business, government, and non-profit institutions have expressed difficulty finding personnel with appropriate training in cyber security tools. SISMAT will draw undergraduate students from other New England colleges, train them about cyber security in a short course at Dartmouth, and place them in corporate internships for the summer of 2008. As a side effect, SISMAT provides opportunities for secure systems research and development to traditionally underrepresented student populations, and facilitates the development of secure systems curricula at other academic institutions.

SECURING THE eCAMPUS 2.0
Building a Culture of Information Security at an Academic Institution

O n October 10th, the Institute for Security Technology Studies (ISTS) and Dartmouth’s Peter Kiewit Computing Services co-sponsored their first annual conference on campus information security entitled, “Securing the eCampus 2.0: Building a Culture of Information Security in an Academic Institution.”

The purpose of the conference was to bring together CIOs, CISOs and others responsible for information security from colleges and universities throughout New England and New York. The main topics for discussion included strategic planning and decision making for information security in higher education, IP ubiquity, data security and the unique challenges posed to academic institutions, and security awareness.

The conference drew a core group of participants from area colleges as well as some IT managers from the local K-12 school districts. Eight presenters and a round table discussion made for a very full day.

David Kotz, the Executive Director of ISTS, kicked off the day by providing an historical overview of Dartmouth’s impact on computing, from the 1950s when John McCarthy coined the term “artificial intelligence,” to the mid-1960s when John Kemeny and Thomas Kúrtz created the BASIC computing language, to 2001 when Dartmouth became the first Ivy League school to deploy a campus-wide wireless network.

The morning sessions focused on the importance of engaging the various groups within the academic community, not just the IT professionals, and discussed the importance of educating the whole community in information security. Rey Junco, of Lock Haven University and author of Connecting to the Net Generation, helped provide context about the mindset of today’s college students and how they interact with technology. He was followed by Tracy Mitrano of Cornell, who contrasted the need for information security with the need for privacy protections. Her presentation included information about the university’s role in supporting national security (e.g., through the Patriot Act) and a staunch defense of academic freedoms.

Tom Quinn of Goldman Sachs focused back in on the student and described the type of person and the background and expertise that person must have that is looking for a job in the corporate world. Bob Du Charme rounded out the morning session by providing the audience an overview of Cisco Systems’ efforts to train university IT faculty and staff in information security through their “boot camp” approach.

Continued on page 2
continued from page 1

Afternoon sessions explored institutional challenges and practical solutions with discussions on regulatory developments, privacy issues, and approaches to building cross-campus collaboration. Matt Brill of the Washington, DC firm Latham and Watkins, and advisor to EDUCAUSE, provided a detailed description of the Communications Assistance for Law Enforcement Act (CALEA) and what academic IT professionals need to be aware of in carrying out their responsibilities. Annie Antón, a professor at North Carolina State University and head of theprivacyplace.org provided some eye-opening examples of the threats to privacy that we face on a regular basis. She also reminded us all of the responsibilities colleges have in protecting the privacy of their students, faculty and staff.

Dartmouth’s own Computing Services and ISTS collaborative security team next led a round-table discussion on its efforts to improve information security on campus. They provided an overview of the software capabilities developed in-house that would be made available to all campus IT communities to enable easier and more thorough vulnerability assessment of campus-scale networks. Possibly more significantly, they demonstrated the strides they had made and success they had achieved as a result of bringing all parties (faculty, staff, graduate and undergraduate students) into the discussion.

Mich Kabay and Peter Stephenson of Norwich University provided the closing presentation. Mich outlined the constant and varied threats that all areas of the university must protect against and illustrated that information security was as much, if not more, of a “people problem” as a technical problem. Peter followed with a case study that illustrated just how detrimental the disregard for the simplest of security practices can be.

David Bucciero, Dartmouth’s Computing Service’s Director of Technical Services, closed the day by thanking all for the great presentations and resulting discussion and queried the audience for their interest in making the conference an annual event. The response was resoundingly in the positive.

The full agenda, speaker bios, and several of the presentations can be viewed at: http://www.dartmouth.edu/comp/about/conferences/security/.

Cyber Security Camp

This June, Dartmouth College hosted a one-week half-day Cyber Security Camp with 12 high school students representing four Upper Valley high schools. As a continuation of the previous summer’s pilot, which included a cyber security component in the robotics camp program, the focus of this camp was on security awareness in the community and to encourage students to practice security in their everyday lives. There was no charge for this camp, which was sponsored by the Office of the Provost, the Department of Computer Science and ISTS.

Through a series of hands-on activities, students experienced the importance of using strong passwords to protect their accounts; explored the use of cryptography to secure their email and instant-message communications; applied Photoshop tools to increase their awareness of (digital) image forgeries; and experimented with Tor as a way to protect their privacy through anonymizing networks. Ethical and legal concerns were an underlying theme that included an activity featuring candid discussions on topics such as digital rights management and case studies of real-world litigation relating to cyber crime. The week’s agenda included presentations by Professor Sean Smith and Sergey Bratus, senior ISTS researcher; a visit to the Rauner Library, led by librarian Ann Perbohner to view related archives; and tours of the computer science and Kiewit computing facilities.

The topics and content were identified and developed over a period of many months by a team of Dartmouth instructors, including: Apu Kapadia (Lead Instructor and ISTS Research Fellow), Jonathan Barlow (Thayer doctoral candidate), Patrick Tsang (computer science doctoral student) and Kimo Johnson (Guest Instructor and computer science doctoral candidate). The effort was developed and led by Suzanne Thompson, visiting scholar and director of the program.

For additional information on the summer robotics and cyber security program see http://www.cs.dartmouth.edu/robotcamp or contact Suzanne Thompson, program director at Suzanne.Thompson@Dartmouth.edu.
Profiles

With this Newsletter, ISTS re-introduces our affiliate profiles. With a new book scheduled for release on 30 November 2007 by Addison Wesley Professional, we focus on Professor Sean Smith, co-author of *The Craft of System Security*. Professor Smith teamed with his former student, John Marchesini on the book, which is receiving advanced critical acclaim. As described by the publisher:

*Whether you’re a security practitioner, developer, manager, administrator, or user, this book will give you the deep understanding necessary to meet today’s security challenges—and anticipate tomorrow’s. Unlike most books, The Craft of System Security doesn’t just introduce the modern security practitioner’s toolkit: it reveals why each tool exists, and demonstrates exactly how to use it to solve real problems.*

What are your primary research interests?
How do we build and deploy trustworthy systems in the real world?

For a long time, I’ve looked at how we can increase trustworthiness by changing the hardware architecture at the bottom; more recently, I’ve been looking at how we can capture and express human and organizational trust via usable public key cryptography.

What are you working on at ISTS?
Right now, I’m working on projects related to these interests: using hardware tricks to improve security, exploring authorization and access-control requirements and practices in real-world enterprises, and using traditional and experimental PKI to try to meet these requirements.

How did you decide to become a computer scientist?
It was a roundabout journey. As a kid, I played around with digital electronics. It was the early days of microprocessors; the only way a kid could afford to get a computer was to build one, but it was actually possible to build one. And you could get all the way down to the bottom of it all.

I went off to college intending to be an electrical engineer, but switched to theoretical math, because it let you get all the way down to the bottom of it.

For grad school and beyond, I went back to computer science and computer security, because it was all brand new—and exploring it let you go from social and psychological issues, to mathematical foundations, to hardware; you can go all the way to the edges, in all the directions. If the field ever settled down, I think I would have to change careers.

What advice would you offer to someone contemplating going into your field?
Computing works because of things that happen on many levels: humans, user interfaces, software, operating systems, languages, algorithms, hardware—not to mention economics and policy. To be most effective, you need to be able work on many levels of abstraction at the same time. Try to develop that skill!

Of what professional accomplishment are you most proud?
You probably expect me to say something about technology here. But I’m more proud of the positive affirmation from the students—things like graduating seniors naming my classes “favorites” or grad students replacing the furniture in my office with livestock (as a prank to celebrate tenure).

When I left industry, I wasn’t sure that would work out!

What are your favorite non-work activities?
Cycling, cross-country skiing, and trail running.

What was the last book you read?
“The Secret Life of Lobsters.” I’ve also been reading a lot about Anasazi ruins recently.

What do you most like about Hanover or Dartmouth?
Everything I like to do is just outside the front door.

What do you think is the best-kept secret about Dartmouth?
The culture here that fosters collaboration across disciplines.

ABOUT THE BOOK:
At the dawn of the Web, I ended up as part of a team at Los Alamos National Laboratory doing security analysis and design for a large number of real-world systems (mostly public sector). In this experience, two things in particular struck me: the unexpectedly broad range of aspects of the problems our clients were facing, and the unexpectedly large range of the toolkit we could use to help. Subsequently, I was continually dismayed at the narrowness of much security expertise. It’s a broad problem, and we need to look at it broadly.

When I started teaching a security course at Dartmouth in the spring of 2001, I tried to do something about this—to expose students to the breadth of the items in the security toolkit, and to prepare them to be effective security artisans and responsible cybercitizens. I couldn’t find a textbook out there that gave a sufficiently broad approach, so I ended up developing my own material. My student (and former ISTS denizen) Dr. John Marchesini, with extensive security attack and defense experience, joined on, and we turned it into this book.

We crafted the book for students and professionals who may never take another course in security, but want to know what the tools are, what to think about when using them, and what the basic principles are that underlie it all. We didn’t want to cover just hacks and patches du jour, or cryptographic protocols—rather, we wanted to communicate the whole picture, and to communicate things that will still be useful five years from now.
Several of our ISTS affiliates spent time in corporate internship and fellowship roles this summer. Ph.D. students Chris Masone and Sara “Scout” Sinclair spent their summers on the West Coast; Chris working as a software engineer at Google Headquarters in Mountain View, CA and Scout interning at Intel Corporation in Oregon. ISTS postdoctoral fellow Apu Kapadia spent a month with Microsoft Research in Bangalore, India. Scout and Apu highlight their experiences below.

This summer, ISTS Fellow Apu Kapadia spent the month of August as a visiting researcher at Microsoft Research India (MSRI), Bangalore.

Apu has been collaborating with MSRI’s Rigorous Software Engineering group to develop an identity management scheme that enables the controlled disclosure of private information between two parties. He sees applications of this scheme from conventional web-based authentication to interaction between mobile-phone users. Apu’s collaborators are Prasad Naldurg (MSRI) and Karthik Bhargavan (MSR Cambridge).

Apu’s experience at MSRI, where he met many fine researchers, including student interns from all over the world was rewarding. Overall, Apu highly recommends that anybody who can afford the time should visit India for its exciting research (and travel) opportunities.

Apu was also pleasantly surprised to see ISTS Executive Director David Kotz during his visit to Bangalore!

In holding with the ISTS goal of educating security experts through multidisciplinary collaboration, graduate student Sara “Scout” Sinclair supplemented her Ph.D. studies this summer by interning with the Network Technology Laboratory of the Intel Corporation. Intel has supported a number of ISTS-affiliated projects in recent years, and Sara was recruited by Victor Lortz and Jesse Walker to build upon her Intel-sponsored research on access control for mobile devices.

Sara joined Intel at the Hillsboro, Oregon, campus, where she had the opportunity to interact with professionals from many parts of the corporation, including high-ranking technical managers, research scientists from several disciplines, recent college graduates, and fellow interns from institutions around the world. She also was able to travel to Intel’s Santa Clara campus, where she visited Dartmouth and ISTS alumna (and her former officemate) Dr. Meiyuan Zhao, who started work at Intel following her graduation in 2005. In her free time, Sara was also able to visit extensively with her aunts and their families, who all live in the Portland area.

Sara’s research at Intel focused on access-control systems for consumer environments, where the “administrators” are average users without particular security expertise. She identified a number of factors that inhibit growth of technology that is rapidly taking hold in enterprise settings, and drew on her back-ground in human-oriented system design to develop a strategy for technology leaders and standards bodies to provide consumers with solutions that both secure their resources and are easy and flexible to use. Sara’s summer work has been published as a whitepaper within Intel, and she is collaborating with her Intel mentors during the fall term to prepare the results for external publication.
New Publications


Welcome

Xia Zhao joined ISTS as a research fellow in September. Xia’s research interests span economic and organizational aspects of information systems and electronic commerce. She specializes in information security and risk management within and/or across organizations. Currently, she is working on an ISTS research project entitled “Information Risk in Data-Oriented Enterprises.” She received her Ph.D. in information systems from the University of Texas at Austin, and her MS in control theory and control engineering and BS in automation from Tsinghua University.

In September 2007, Mirco Musolesi joined ISTS as a Postdoctoral Research Fellow in the Department of Computer Science, where he is also a member of the Sensor Networks Group. Currently, Mirco is working on the MetroSense Project, which is a collaborative project between Dartmouth’s ISTS, Computer Science, and the Thayer School of Engineering, Columbia University’s Electrical Engineering Department, and Intel Corporation and Nokia Research. MetroSense is a new wireless sensor edge network for the future Internet based on the concept of “people-centric sensing” at scale. Mirco received his Ph.D. in Computer Science from University College London in May 2007 and a Laurea in Electronic Engineering from the University of Bologna in December 2002.

Minho Shin earned his Ph.D. in Computer Science from the University of Maryland at College Park in November 2007. His graduate research focused on the performance and the security of wireless networks. He received a B.S. in Computer Science and Statistics from the Seoul National University in 1998 and a M.S. in Computer Science from the University of Maryland at College Park in 2003. He joins ISTS as a Postdoctoral Research Fellow with David Kotz for the MetroSense project.
Distinguished Speakers

November 6, 2007
“Disruptive Technologies for Information Assurance”
Carl Landwehr, Intelligence Advanced Research Projects Activity.

October 22, 2007
“Topics in Mesh Security”
Jesse Walker, Intel Corporation.

October 18, 2007
“The Challenges of 21st Century Information Assurance R&D - A Perspective from a Large Scale Global Enterprise”
Ming-Yuh Huang, The Boeing Company.

Upcoming Speakers

February 12, 2008
Stefan Savage, University of California, San Diego (UCSD).

TBD
Hari Balakrishnan, Massachusetts Institute of Technology (MIT).

TBD
Donna Dodson, National Institute of Standards and Technology (NIST).

For more information about our speaker series visit our website at www.ists.dartmouth.edu/events.php.