A Message from the Director
Developing Tomorrow’s Security Experts

A key component of both the Comprehensive National Cybersecurity Initiative (CNCI) and the President’s Cyberspace Policy Review and now the central tenet of the National Initiative for Cybersecurity Education (NICE) is to strengthen the future cybersecurity environment by expanding cyber education and the recruitment, training, and retention of cybersecurity professionals. The US Cyber Challenge Program is looking for 10,000 Americans to fulfill the demand in government alone, while the federal government’s CIO Council Net Generation Report estimates an increase of nearly 1 million IT jobs in the economy as a whole over the next decade.

Meeting the demands for the cybersecurity workforce will require us to recognize the need to address the diversity of that workforce at the same time. Currently, women earn less than a quarter of the degrees conferred for Computer and Information Sciences and Engineering in the United States. Similarly, African-Americans and Hispanics are underrepresented on college campuses in general, and Hispanics are also underrepresented in Computer and Information Sciences and Support Services majors.

The goal to increase the cyber workforce should go hand-in-hand with the need to expand the diversity of IT students and workers. Indeed, the goals are mutually reinforcing – we will more easily expand the cyber workforce if we increase the pool of technically educated and trained workers by increasing the number of women and ethnic-minority students in computer science and engineering.

As part of the ISTS mission to educate the next generation of information security experts, we have a number of initiatives to address the dual issues of diversity and cyber training of the IT workforce. The AUK-Dartmouth video-conversation among women computer science students from Kuwait and the US initiated a cross-cultural discussion of gender and computer science. In addition, our speaker series this year will address a variety of diversity issues in IT and cybersecurity. Finally, as we begin accepting applications for both the IASP scholarship program and the SISMAT summer program, diversity will be one of our key objectives.

How Do You Grow Computer Security?

The need for information security specialists increases each year, with the federal government alone seeking to fill thousands of positions. However, the demand for those with the skills necessary to enter these jobs far exceeds the supply. One means of closing this gap is through promotion of focused educational initiatives.

At Dartmouth, ISTS manages three such efforts: the Secure Information Systems Mentoring and Training (SISMAT) program; the Department of Defense’s Information Assurance Scholarship Program (IASP); and the Cyber Security Summer Camp. In the articles that follow, we address recent news regarding each program and provide reports from our recent ISTS-Neukom Institute Internship Grant recipients.

SISMAT 2010...and 2011 and 2012

Begun in the summer of 2008, the Secure Information Systems Mentoring and Training (SISMAT) program has graduated 23 students from 10 universities, engaged 15 faculty mentors, and encouraged expansion of the program’s methods through presentations at various conferences.

The SISMAT program takes a unique approach to teaching students about security. SISMAT faculty leaders Michael Locasto and Sergey Bratus have developed the course utilizing, what they call, the “hacker curriculum”. They define “hacking” as the ability to question and verify trust assumptions in the design and implementation of computer systems, rather than any negative use of such skills. Based on the belief that students will learn better and more about information security by teaching from this perspective, Professors Locasto and Bratus encourage their students.

Inside This Issue

SISMAT 2010... and 2011 and 2012 ................page 1
Information Assurance Scholarship Program ..... page 2
2011 Cyber Security Camp ............................. page 3
ISTS-Neukom Institute Internship Grants...... page 3
Securing the eCampus 2010 ........................... page 5
Postdoc Profiles ............................................. page 6
AUK-Dartmouth Women in CS Discussion .... page 7
NSF Award for “Wireless Fingerprinting” ....... page 9
to “think like a hacker” by trying to consider all of the things that could be exploited in a system or network.

Through the SISMAT program, students participate in an intensive two-week security training course in mid-June, followed by a summer internship (acquired with the help of SISMAT organizers), and a semester or year-long independent project at their home institution. All of this is free-of-charge to accepted students.

Faculty participants serve as mentors to the students throughout their involvement in SISMAT, and as academic advisors for independent study. They also collaborate with the SISMAT internship supervisors in identifying areas in which regional institutions can develop their programs to better prepare students to assume security positions upon graduation.

Throughout the course of the year, leading up to SISMAT, Professors Locasto and Bratus promote the program to interested audiences. In March 2010, Locasto presented the paper “Teaching the Principles of the Hacker Curriculum to Undergraduates” at SIGCSE 2010 (Special Interest Group on Computer Science Education) in Milwaukee, Wisconsin; the premier CS education conference. Response to the paper was strong and this year Locasto will host a “Birds of a Feather” session at SIGCSE 2011 to further develop and promote SISMAT techniques.

This year’s SISMAT course was run June 22nd to July 2nd. Eight students from a diverse set of schools, including four new participating institutions, were accepted into this year’s program. While the format for the course followed the basic structure of the previous two year’s offerings, the course materials and labs for this year’s program were redesigned and refreshed.

Over the course of 10 days, the students participated in morning lectures and afternoon labs. Each night the students were required to do an extensive amount of reading to prepare for the next day’s activities. Guest lecturers were also part of the 2010 curriculum. Guests included: Doug Madory of Renesys Corporation; Steve Nyman, Dartmouth’s Chief Information Security Officer and previous CISO of Pfizer; and Adam Goldstein, Dartmouth’s Security Engineer and a co-leader of the Cyber Security Initiative. As in previous years, the class also took a field trip to Dartmouth’s networking services machine room, led by Dartmouth’s Director of Technical Servic-
es, David Bucciero.

For the first three years of its existence, the Department of Homeland Security’s National Cyber Security Division (NCSD), with supporting funds from the Department of Defense’s Information Assurance Scholarship Program, funded SISMAT. This year, SISMAT was awarded funds by the National Science Foundation’s (NSF) Course, Curriculum, and Laboratory Improvement (CCLI) program (now known as Transforming Undergraduate Education in Science, Technology, Engineering and Mathematics, or TUES) that will ensure the program runs for at least two more years while laying the foundation for a curriculum and sample labs that can be shared with a wider audience.

For more information on the SISMAT program, see the ISTS website and look for SISMAT on the “Events” page. Recruiting has begun for 2011.

The Information Assurance Scholarship Program

Each year the Department of Defense (DoD) seeks rising junior and senior undergraduate and graduate students who are interested in concentrated studies in information assurance.

Students selected for the program receive full scholarships and the opportunity to participate in internships in government. Scholarships include funding for tuition, books, fees, labs, equipment and a stipend to cover room and board ($14K for undergraduates and $19K for graduate students).

Acceptance requires the student to agree to one year of service to the DoD, upon graduation, for each year of scholarship received, in addition to participation in an internship.

In the first year it was offered on campus (the academic year 2009-10), Dartmouth hosted two IASP scholars. One scholar graduated last year and is now working within the Defense Department. The other scholar will conclude his studies in June 2011 before going on to his job next summer. He provides an update on his experience in the following paragraphs.

*The Information Assurance Scholarship Program (IASP) has provided me with a great opportunity to focus on cybersecurity related studies while in college. In addition to providing a scholarship for my
Education

ISTS-Neukom Institute Internship Grants

In addition to the educational opportunities noted above, ISTS and the Neukom Institute for Computational Science co-sponsor an internship each term at Dartmouth College. The funding is available for undergraduates on their leave terms to gain work experience, advance research skills, or become familiar with a new area of information technology.

Applications are now being accepted for spring term funding. The due date is February 2nd. Applications for the summer term will be due on April 27th. For more information on the program go to the “Opportunities” page on the ISTS website. Read the following two articles by Lauren Rosenbaum ’11 and Emma Smithayer ’12 for descriptions of previous intern experiences.

2011 Cyber Security Camp

In the summer of 2004, a Summer Robotics Camp Program was piloted for middle school students in Dartmouth College’s Department of Computer Science under the leadership of visiting scholar, Suzanne Thompson. In the following years, the Department of Computer Science, the Neukom Institute, and the Provost’s Office of Dartmouth College sponsored the program, so that there was no charge to the students. Over time the scope of the program was expanded to include an innovative cyber security program for high school students while continuing with its hands-on learning approach guided by Dartmouth student instructors.

This year, recognizing the program’s past success in attracting talented youth, the Department of Defense, through the Information Assurance Scholarship Program, awarded Dartmouth funds to once again run a computer security focused camp for high school age students. Suzanne and a team of graduate and postdoctoral students have begun to develop a cross-disciplinary security course that will take place next summer. Please check the ISTS website this spring for more information.

P2P Microfinancing in Kenya

By Lauren Rosenbaum ’11

Successful development strategies must adapt to the breathtaking speed at which information and communications technology is growing in Africa in order to harness its potential for meaningful change. The Neukom Institute and Institute for Security, Technology, and Society internship grant allowed me to observe firsthand how technological innovations allow development assistance to reach the world’s poor at a higher speed and volume than ever before. My position was with a recently launched P2P microfinance network called Zidisha (Swahili for “expand”).

Nearly every adult I met in Kenya owned a cell phone, and several had relatively inexpensive phones with 3G browsing capability. Cell phones in Kenya serve not only as essential communication tools, but also as substitutes for banking. Small business owners deposit money into their mobile money accounts in order to carry less cash. Parents living away from their families can send money home instantly, rather than physically shuttling it across the country. Shoppers in local marketplaces who are out of cash can simply send money to vendors. According to the Wireless Federation, a wireless industry research conglomerate, about 51% of adult Kenyans own a cell phone and in July about 11.9 million individuals in Kenya transferred money through M-Pesa, the country’s leading mobile money provider operated by
the company, Safaricom.

International peer-to-peer lending platforms use information and communications technology to connect globally conscious individuals with poor people in the developing world. Partnering with umbrella institutions like Kiva and MYC4 allow small microfinance organizations to access funds that they would be unable to raise independently. Nevertheless, the ease with which big peer-to-peer organizations channel funds to borrowers glosses over some messy and unflattering realities of the microfinance process.

Julia Kurnia, the founder and director of zidisha.org, wanted to develop a microfinance model that harnessed the powerful fundraising capability of a peer-to-peer network without the high transaction costs associated with traditional microloans. Kiva’s field partners charge an average of over 37% interest on their small loans according to data provided on their website. Some partners charge much higher interest; Tujijenge Tanzania’s self-reported rate is 98%. MYC4’s entrepreneurs annual interest rates can be as high as 72% and average over 56%.

Zidisha borrowers create loan applications online and post their own comments on their profiles, rather than relying on loan officers to do this work for them (either the borrower, a family member, or a trusted friend must be computer-literate in order for them to qualify for Zidisha loans). Borrowers receive loans and make payments through their cell phones using mobile money rather than physically going to a bank or submitting payments to loan officers. Beyond keeping interest rates low, Zidisha’s model ensures that lenders’ money actually gets to borrowers. Because payments are electronic, borrowers’ repayment records are updated the same day that they are made. Their repayment record combines with their commitment to posting comments on their profiles toward their lender approval rating, which can either help or hurt their ability to fund future loans. Borrowers are advised to post comments at least once monthly in order to establish a positive relationship with lenders.

Many people are amazed to learn that I had regular internet access pretty much everywhere I went in Kenya. Using a mobile modem, all I needed was network coverage from my cell provider to be connected. While I was rarely in areas with electricity access, local businesses often own generators that customers can use to charge their cell phones (or in my case, netbook) for a small fee. Because my computer had a battery life of around eight hours, I was able to take it with me on field visits in order to show potential clients exactly how Zidisha loans worked. I was also able to communicate regularly with my supervisor in the US and to update my weblog that I used to chronicle my life and work in Kenya.

Zidisha is still a young organization, with only 42 current borrowers. We are nowhere near accumulating a lending base as massive as that of Kiva, which according to its website finances a new loan every 13 seconds. Nevertheless, Kiva was once a small operation with an innovative idea, just like us. It’s exciting to be a part of Zidisha’s growth and I thank the Neukom Institute and the Institute for Security, Technology, and Society for giving me the opportunity to do so.

Laptops for the Children in Uruguay

By Emma Smithayer ’12

With the generous funding of ISTS and the Neukom Institute, I had the opportunity to spend spring term in Montevideo, Uruguay, working with several local nonprofits supporting Uruguay’s one-to-one computing initiative, Plan Ceibal. Uruguay purchased 400,000 of the budget laptops designed by One Laptop Per Child (OLPC) and by the end of 2009 completed distribution of the computers to all public elementary school students in the country. The result is that a third of the households in the country have one of the laptops (called “XOs” internationally and often “Ceibalitas” in Uruguay). As of October 2009, about 1,900 of the 2,332 schools had Internet, and that number is steadily increasing. But the real work of the plan—integrating the XOs in a way that maximizes the educational benefits—is just getting started.

ceibaJAM! is a nonprofit that recruits volunteers to write applications for the XOs and tests them in schools. Blogging Desde Infancia (“Blogging Since Infancy”) is a related group that runs blogging workshops and competitions for kids and teachers around the country. I spent most of my time with these two groups.

Each group organized visits to schools for research and workshops, where I got to observe the wide range of Plan

Laptops for the Children in Uruguay continued on page 7
Securing the eCampus 2010

Security awareness, metrics, cloud computing, cybercrime, and more were on the agenda for this year’s 4th Annual Securing the eCampus conference held in July. ISTS, along with Dartmouth’s Kiewit Computing Services Department, once again welcomed IT leaders from colleges and universities across the northeast to participate in the three-day conference. More than 70 Chief Information Officers (CIOs), Chief Information Security Officers (CISOs), and other academic IT security leaders participated.

This year’s format included the traditional day of lectures and half-day of break-out sessions, but also introduced an opening afternoon of training sessions led by Dartmouth personnel. Steve Nyman, Dartmouth’s CISO, led a session on developing university-wide security policies, while Adam Goldstein, Kiewit’s Security Engineer, led a session that considered security in the cloud. The sessions were well-attended as both topics are at the forefront of most universities’ focus for security planning.

Day two included a full-day of lectures and a panel discussion on the pros and cons of cloud computing. Greg Jackson of EDUCAUSE kicked off the day with a discussion on security and privacy policies and how an educational institution can best align priorities. Cormac Herley of Microsoft Research then gave a presentation questioning the effectiveness of current security advice for the average user, which produced a rather rousing discussion.

Matt Devost, an independent consultant and security expert, provided perspective on cyber threats generally and how they can effect highly IT-dependent organizations. Matt was followed by Michael Kaiser, the Executive Director of the National Cyber Security Alliance (NCSA) who gave an overview of the many initiatives his organization is helping to implement to raise security awareness.

Attorney Ray Beckman advised the audience on how universities should respond to RIAA subpoenas while protecting their (and their students’) legal rights, noting the complexity involved and the need for careful assessment given the untested landscape that is this new area of litigation. Author and attorney Frederick Lane concluded the day with a review of the right to privacy in the context of the digital age.

The last day of the conference provided participants the opportunity to gather in break-out sessions to discuss a variety of topics including: botnets; social media and the college student; implementing a “hacker curriculum”; and eDiscovery.

ISTS and Kiewit have begun planning for another year of eCampus. Please check the ISTS site regularly for “save the date” notices. eCampus 2011 will likely take place in late July. The program committee is always interested in ideas for topics to be covered. Please email any recommendations to info.ists@dartmouth.edu.

National Cyber Security Awareness Month

While it’s a good idea to be “cyber aware” at all times, the National Cyber Security Alliance (NCSA) works hard to get the message out through a national campaign each October. This year Dartmouth and ISTS signed on with numerous organizations to endorse National Cyber Security Awareness Month and offered events promoting security awareness. This October we sponsored talks by Steven Davis, the CEO of IT GlobalSecure, Inc., who spoke on gaming security and Professor David Wall, a criminologist from Durham University (UK), who presented on cybercrime. Both of their presentations are now available on the ISTS YouTube playlist.

Be sure to also visit the Securing the eCampus 2010 conference pages on the ISTS website and view NCSA Director Michael Kaiser’s presentation given on the Dartmouth campus this past July.
ISTS welcomed two new postdoctoral researchers this summer.

**Jacob Sorber, PhD**  
SHARPS Project

Jacob joined ISTS in 2010 as a postdoctoral associate, working with David Kotz on improving the security and performance of mHealth sensing systems. He completed his PhD at the University of Massachusetts Amherst, where he explored language and runtime system-level techniques for building mobile sensors that are both energy-aware and self-managing. Jacob also completed a B.S. in Computer Science at Brigham Young University, in 2002.

**What are you working on at ISTS?**  
I'm working on the Strategic Healthcare IT Advanced Research Projects on Security (SHARPS) project, exploring the use of mobile sensing systems in medical and healthcare sensing environments. I am initially trying to protect the integrity and confidentiality of medical sensing data and computation residing on devices like cell phones that are vulnerable to software-based attacks.

**What are your primary research interests?**  
I'm broadly interested in mobile computing systems and wireless sensor networks, and my research focuses on making these systems more flexible and efficient, more secure, and easier to use. I intentionally keep this focus broad, so that I can bring together ideas from areas like networks, operating systems, programming languages, and security. I also love working with scientific disciplines outside of computer science, like biology and medicine.

**How did you decide to become a computer scientist?**  
I have been writing software for most of my life. I started programming out of curiosity when I was 11 years old, and so, in college it was a natural specialty. Still, I've always been more of a scientist than a developer. I love trying new things, running experiments, and pushing the limits of my understanding. I had the opportunity to do some research during my last year as an undergraduate student at BYU, and I knew it was what I wanted to do.

**What advice would you offer to someone considering going into your field?**  
Computer science is a great field, but many students make their career decisions based on very narrow stereotypes and misconceptions. Computer science is really one of the most flexible and interdisciplinary fields out there. In the past decade I have used my computer science degree to design radar sensors, analyze roadway traffic, help automotive technicians fix cars, put content on the evening news, and study endangered tortoises. Now, I'm using it to help people live healthier lives. The opportunities are endless, but too few students give it a chance.

**Which professional accomplishment makes you most proud?**  
It's hard to choose just one. It's probably a 3-way tie between designing the very first energy-aware programming language (Eon); deploying a mobile testbed of sensor devices carried by tortoises (UMass TurtleNet); or becoming the resident turtle/tortoise expert in the mobile systems and sensor networks communities.

**Juhee Kwon, PhD**  
TISH Project

Juhee joined the Center for Digital Strategies, Tuck School of Business in 2010 as a research fellow, working with M. Eric Johnson on studying healthcare security management. She earned a PhD from Krannert School of Management, Purdue University in 2010. Prior to joining the Purdue PhD program, she worked at Samsung Electronics. She received a master's degree in Information Management Systems from Carnegie Mellon University in 2003. Juhee completed a bachelor's degree in Microbiology from Kyungpook National University in Korea.

**What are you working on at ISTS?**  
I am involved in the Trustworthy Information Systems for Healthcare (TISH) project, and working on how security-related IT disruptions drive appropriate security investment/diligence within a healthcare organization. Statistical methods are employed to analyze the data collected from various healthcare databases. As subsequent issues, I also plan to study how the lack of security (or poorly implemented security) erodes patient care and healthcare operating continuity/efficiency.

**What are your primary research interests?**  
My primary research interests are in information risk management. My doctoral dissertation studied how CIO/TMT structure influences information risk management in a firm and how successful information risk management improves consumer trust on electronic markets. Now, I explore many facets of information risks in the healthcare sector and focus my efforts on studying how information risk is evolving and estimating the economic impact facing patients, providers, and payers.

**Which professional accomplishment makes you most proud?**  
I would have to say that my proudest accomplishment is completing a doctoral degree, as it shaped my understanding of hard work and showed me how much I can achieve when I test my own limits. This achievement is meaningful to me because choosing graduate school over industry where I had been building a career path my whole life was one of the toughest decision that I had to make.
Ceibal’s effects. The events often had a palpable sense of excitement. Students and teachers alike enthusiastically came to school after hours for computer workshops. On one trip, we met disabled students who were thrilled that they could play a computer game by moving a lever with their heads—possible only because volunteers had written an accessible version. It was great to see kids using programs that ceibalJAM!’s volunteers had helped build, and to know that I was contributing to that progress.

I also worked on several projects independently. I translated some documents, like a history of ceibalJAM!, from Spanish to English, allowing the groups to increase international collaboration. I filmed various ceibalJAM! and Blogging Desde Infancia events—programming “jams” for volunteers and visits to schools—and then edited them into short videos to post on YouTube, to help publicize the groups’ activities. I tested several projects in development, like a blog site called EduBlog (a kid-friendly version of Blogger or WordPress), and helped create the plans to improve them. Later in the term, I started work on a project called Blog-Pals that involves using games and blogging to teach kids some beginning English and connect them to English-speaking kids learning Spanish.

The experience sparked more questions than it answered for me about technology’s effects on a society. After all, the goal is not merely to turn out computer literate students. When these kids grow up, will they be more likely to go to college, learn other languages, start businesses, be involved citizens? Will it change their opinions of social norms, or of Uruguay’s place in the world? Will it revitalize Uruguay’s economy, or just accelerate the brain drain? Will socioeconomic achievement gaps widen or narrow? Questions like these continue to inspire my interests in technology, and I am grateful for the opportunity to learn so much about this groundbreaking project.

An “Undeniable Connection”: Young Women From Kuwait and the U.S. Find Common Ground as Computer Science Majors

By Tiffany Pollack ’10, Public Affairs

It was 9:15 a.m. in Hanover and 4:15 p.m. in Kuwait City on October 21 when two groups of young women—one at the American University of Kuwait (AUK) and one at Dartmouth, talked about the reasons they chose to major in Computer Science. Facilitated by the Dartmouth College-American University of Kuwait Project, the Institute for Security, Technology, and Society (ISTS) at Dartmouth and the Dartmouth Women in Science Project, the conversation took place in real time using videoconferencing technology in the Dartmouth Center for the Advancement of Learning (DCAL), and the Information Technology Department and the Library at American University of Kuwait (AUK).

The videoconference highlighted a growing list of activities that take place as part of Dartmouth’s relationship with AUK, now in its seventh year. One aspect of that relationship, the AUK Faculty Fellows Program, brings faculty members to Dartmouth to work with counterparts in Hanover. AUK Assistant Professor of Computer Science Amir Zeid visited Dartmouth in summer 2010 to work with George Cybenko, the Dorothy and Walter Gramm Professor of Engineering. Struck by the relatively low proportion of women studying Computer Science at Dartmouth and elsewhere in the United States—in sharp contrast to AUK, where a high percentage of Computer Science majors are women—Zeid approached Denise Anthony, Associate Professor and Chair of Sociology and Research Director at ISTS — with the idea of launching joint research on the issue, beginning with a conversation between students at the two institutions.

“I began my formal research on how cultural issues affect women’s enrollment in Computer Science academic programs in May 2010, using Kuwait as a case study,” said Zeid. “The videoconference was a great learning experience for all of us, and I hope it leads to a long term research collaboration with Dartmouth.”

“All of us truly felt that we were sitting in one room,” added Rehab El Bahey, who moderated the conversation in Kuwait. El Bahey is a coordinator in AUK’s Arabian Heritage Project. On the day of the videoconference, she worked with Christina Chen ‘10, a Dartmouth student in Kuwait for the fall term as an intern at AUK. “The flow of the discussion and the similarities in thoughts and experiences eliminated all time, place, and cultural barriers”, observed El Bahey.

One Dartmouth participant, Shloka Kini ‘13, found that the conversation revealed both similarities and cultural and educational differences between her undergraduate experience and that of the women who attend AUK. “It would be mutually beneficial to keep in contact [with this group],” she said, “not only to continue the conversation but to build bonds with other women for future collaboration.” She described the session as “an undeniable connection,” adding, “Perhaps in the future, we will all have changed the world with this conversation about girls in Computer Science.”
“The lack of gender diversity among computer scientists, as in math, engineering and science more generally, is a significant concern in the United States, and here at Dartmouth,” said Denise Anthony. “Collaborations like this Dartmouth-AUK videoconference provide an incredible opportunity for women in computer science to learn from, and support, one another. We hope this will turn into an ongoing collaboration.”

Videoconferencing between AUK and Dartmouth has become a continuing aspect of the institutional collaboration. Web technology allows participants on both sides of the world to erase the physical distance between them. Previous sessions have involved the institutions’ respective Writing Programs, a joint session of a Dartmouth Anthropology and an AUK Comparative Literature class, and a student-to-student presentation at Dartmouth’s first Student Conference on Global Learning, sponsored by the Dickey Center for International Understanding.

The American University of Kuwait, established in 2003, is a liberal arts institution, based on the American model of higher education. Dartmouth has worked with AUK since its founding under the terms of a Memorandum of Understanding that involves faculty, students, and staff in both locations. Dartmouth experts in engineering, information technology, library sciences, communications, governance, and other areas routinely visit Kuwait while students, faculty, and staff from Kuwait travel to the United States to work with their counterparts at Dartmouth. Since the relationship began, the two institutions have steadily deepened and expanded their partnership, creating a dynamic, evolving, and unique cross-cultural collaboration.

For student participant Shloka Kini’s reflection on the discussion, read the following article.

An Atypical Day in the Life of Computer Science Student Shloka Kini ‘13

During the Cross-Cultural Conversation, one saw an amazing thing happen: a connection. An undeniable connection found only through the medium of computer science had suddenly brought young women from different cultures, different upbringings, and different lifestyles together. It was amazing the variety of ways in which one major ultimately became the defining factor in the lives of so many women. One woman from Kuwait recounts being interested in films; finding them too hard, she opted for computer games and fell into computer science. Another girl graduating this year from Dartmouth expresses her deep-rooted background in computer science, coming from a community where many adults had careers in the field. Another girl was inspired by her mother and decided to follow in her footsteps. As for me, I decided to not choose a major by choosing computer science, which would become very applicable to all fields of study in the future.

In my mind, every field in the world can be as specialized as it wants to be; regardless, every field needs a webmaster, an IT technician, a go-to person for problems with a PC. The computer has been defined by society to be a “geek” tool. For people who are misanthropes, loners, and anti-social, social networking and distant communication in the form of blogs and Twitter become crutches for human interaction. But within this discussion, the walls of stereotypes were torn down, as students realized that computer science can never determine one’s lifestyle especially for women. Having single sex classes in Kuwait, the girls bonded in an unexpected way by being able to see more of each other in their classes. The one commonality in gender discrimination in the field was definitely apparent: the problem was not the gender, the problem was the experience. It seems that unanimously the girls felt inexperienced in the presence of males in their classes who could converse in the jargon, code in the language, and “walk the walk” of a computer “geek.” However, for a girl entering the field as a newbie, it becomes very difficult to relate to the men in the room. I personally encountered a huge experience gap with my first encounter with computer science in high school, when I found myself at a loss during the final project, which was recreating a Pokemon game all of the guys seemed very familiar with.

The remarkable vibe in the room was the incredible strength of the women I met. Each seemed to want to persist in the face of difficulty. Many, I have noticed, find that once a course becomes difficult, it means that it is “not the right field for you.” But for all of these women, difficulty was the perfect fuel to drive them to success in the field. Another interesting perspective was brought up by a girl from Kuwait, who noted that computer science girls in Kuwait were much like the secretary typists from the American 60s. This unique perspective I noticed, made the Dartmouth girls think more about their roles as not only girls but as Americans in the computer science field. In all, the experience was very rewarding and hopefully the discussion will continue; perhaps in the future, we will all have changed the world with this conversation about girls in computer science.
Bratus Receives NSF Award to Research “Wireless Fingerprinting”

In July, Research Associate Professor of Computer Science and ISTS Chief Security Advisor Sergey Bratus was awarded $383K in funding by the National Science Foundation’s (NSF) Trustworthy Computing program for his “Active physical layer fingerprinting of 802.11 and 802.15.4 wireless devices” project. Below, Sergey describes the project’s rationale and focus.

The role local wireless networking technologies play in our everyday lives is set to keep increasing. Wi-Fi (a.k.a. 802.11) networking for laptops and smartphones is already almost ubiquitous, and 802.15.4 technologies (e.g., ZigBee) are becoming the wireless connectivity method of choice for various energy management technologies, in particular “smart grid” and “smart home” applications. They are also likely to be incorporated into all kinds of medical devices that require remote wireless sensing.

But while security of these wireless devices will become increasingly important, there are many known issues that affect security of such technologies. For example, their components are manufactured by many vendors, and often include proprietary features, which, alone or in combination, are known to increase the systems “attack surface”, that is, ways to attack and compromise it. Therefore, it is important to establish the attack surface of these technologies early on, pre-empting the discovery of its vulnerable points by malicious attackers. One of the aspects of this necessary research is mapping out the subtle differences in behaviors between wireless devices and components, in particular looking for those that can be exploited for attack purposes.

In this project, we develop such robust fingerprinting techniques for wireless devices. Our approach uses the less-explored technique of the “active probing” of these devices in the physical (PHY) layer of 802.11 and 802.15.4 networks, which is based on crafting wireless data and control units (the so-called frames) that slightly deviate from the standard, and observing the equipment’s responses.

These responses typically range from ignoring the tweaked input (which is the correct behavior in most situations) or responding to it as if the deviations did not matter (not necessarily standard-compliant, but not offensive from the operator’s perspective), to rebooting or crashing (unexpected, annoying, and hard to explain, from the device’s legitimate operator’s point of view).

However, the most interesting responses include the devices entering states not encountered during normal operation, and sending back some of the internal information not intended to be a part of normal communications protocols. It is these conditions that are likely to have the most impact on security. To empower exploration of the attack surface of actual wireless networks and, in particular, research into active physical-layer testing of wireless devices, we are working on a framework for crafting and injecting “marginally” malformed physical layer signals that correspond to common 802.11 and 802.15.4 frames.

Active fingerprinting methods are the most direct and effective ones, because they allow the administrators to initiate fingerprinting when necessary, probe for a broader range of expected behaviors (and thus increase the attacker’s workload to fake behaviors in order to escape detection), and are easily tweaked (further increasing said workload). Fingerprinting of network devices is also an important capability in the arsenal of the defender of existing cyber-assets, because it helps expose deceptions, which are essential to many modern multi-step network attacks.

We intend our tools to facilitate testing of wireless devices by both vendors and owners, thus improving their trustworthiness, and hopefully avoiding the creation of large installed bases of vulnerable devices in various critical “smart grid” and healthcare technologies, and equipping cyber-defenders with methods of fingerprinting and discovering untrustworthy ones.

Upcoming Speakers

January 25, 2011
Cynthia Rowland, PhD
Executive Director
WebAIM; National Center on Disability and Access to Education
Center for Persons with Disabilities
Utah State University
“Web accessibility in civil society: Persons with disabilities in today’s educational environments”

May 11, 2011
Yoshi Kohno, PhD
Assistant Professor, Department of Computer Science and Engineering at the University of Washington
See the ISTS Website for Upcoming Student Opportunities

**ISTS-Neukom Institute Internship Grant**
Application Deadline: February 2, 2011

**Information Assurance Scholarship Program (IASP)**
Application Deadline: February 7, 2011

**Secure Information Systems Mentoring and Training (SISMAT)**
Application Deadline: February 21, 2011

© Copyright 2010 Trustees of Dartmouth