ISTS Quarterly
Institute for Security Technology Studies
at Dartmouth College

Winter 2005/06 www.ists.dartmouth.edu Volume 2, Number 4

From Our Director

Every great research institution is built on a foundation of great people. Indeed, as I see it, my role at ISTS is to encourage and support a collaborative community of bright researchers who can work together to solve important problems related to cyber security and emergency response

ISTS has the good fortune to have many wonderful people, as you can see in this issue. The Greenpass article on this page indicates the impressive translation of academic research into practical technology, which emerged from a successful partnership between ISTS researchers in Computer Science and Computing Services (Dartmouth's central IT organization), the PKI/Trust Lab, and their work with Cisco and Intel corporations.

We welcome new ISTS Fellows to the Emergency Readiness and Response Research Center. They join three Fellows already in place in the Cyber Security and Trust Research Center. We have a new "Researcher Highlight" feature in the newsletter, this one on Laura Ray. This series will give our readers a chance to know our affiliates better. Researcher Jenny Bodwell reports on her Hurricane Katrina relief work this winter. We highlight the research of our robotics team and one of our senior graduate students, Alex Iliev. Finally, we report on the InterAgency Board meeting, hosted at ISTS this winter.

These articles demonstrate the quality of the work at ISTS and the sense of community that ISTS is fostering through its outreach. We are beginning to see the collaboration and technology deployment that gives our work broader meaning.

The ISTS mission is to strengthen homeland security through research, education, and outreach programs that focus on technology critical for cyber security and emergency preparedness and response. ISTS nurtures leaders and scholars, educates students and the community, and collaborates with its partners to deploy technology to benefit our community and to better understand technology's impact on our security.

Photo: Joe Mehling '69

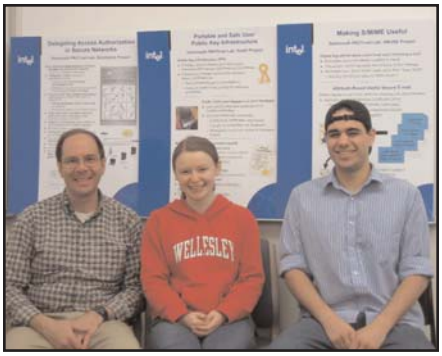
David Kotz

Greenpass demonstration a success

In December, the Dartmouth PKI Lab, funded in part by ISTS, showed off their Greenpass project and described other current research at the Intel IT Innovation and Research Open House, held in Folsom, California. This event for key Intel technical experts and researchers, university partners, and invited press and analysts highlighted current technology trends and challenges and showcased Intel's enterprise and information technology R&D activities.

Dartmouth's Associate Director of Technical Services, Robert Brentrup, installed a working demo of Greenpass, which provides delegated guest access to a secure wireless or wired network using the 802.1x and EAP/TLS protocols. Visitors to the Greenpass exhibit were able to connect their laptops to the Greenpass web application, obtain a guest delegation certificate, and then reconnect their system to the secure network. The installation consisted of a wireless access point, network switch and router, and a laptop running the Greenpass servers. A Greenpass system installation integrated on a bootable Linux CD was used to create the server computer's disk image on site.

Brentrup developed the demonstration and staffed the Greenpass exhibit at Intel along with Ph.D. students Chris Masone and Sara Sinclair. Brentrup reported, "The visitors we talked to were impressed with the Greenpass concept and its implementation. They felt that the system would be a useful ongoing addition to a secure wireless network.They could see applications of it within Intel.



Left to right: Robert Brentrup, Associate Director of Technical Services with Ph.D students Sara Sinclair and Chris Masone

Intel and Cisco Systems sponsored the graduate student research by Nick Goffee and Sung Kim, who developed the Greenpass prototype under the direction of Professor Sean Smith and William Taylor. Additional support from Intel and Dartmouth's ISTS has been committed to refine and augment the prototype and develop an open source distribution of the project. Dartmouth's PKI Lab continues to work with Intel and plans to explore an ongoing deployment of Greenpass and related projects.

For more information, visit http://www.dartmouth.edu/~pkilab/greenpass

Inside

ISTS Hosts Meeting of InterAgency Board Subgroup

On February 8 and 9 ISTS's ER3C was honored to host an information security systems workshop for the Interoperable Communications and Information Systems (ICIS) subgroup of the InterAgency Board for Equipment Standardization and Interoperability Working Group, known as the IAB. The mission of the ICIS subgroup, which consists of emergency responders, government officials and academic researchers from across the country, is to identify available equipment/systems and shortfalls for the coordination, exchange and reliability of information before, during, and after all-hazard events.

ER3C Director Susan McGrath, herself a member of the ICIS subgroup, offered to host the subgroup meeting at Dartmouth "both to show the IAB Dartmouth's capacity in cyber security and to show Dartmouth how easily ISTS can play a supporting role to the nation's emergency responders." The workshop was designed to provide the 19 attendees, including co-chair of the ICIS Christopher Lombard of the Seattle, WA Fire Department, with current information on systems security issues and technologies for emergency response systems including communication and analysis networks.

ER3C Project Lead Dennis McGrath and ISTS Researchers and SANS instructors George Bakos and Bill Stearns presented information on security system design, best practices, equipment guidelines and case examples of information system breaches. This team also moderated a working session where the subgroup members were asked to defend or attack an operational emergency response network. Chris Goggins, President of SDI, Inc., and Don Hewitt, Program Manager at the Terrorism Research Group, also contributed to the presentation. Amy Donohue, Assistant Professor of Public Policy at the University of Connecticut, reported feeling a bit overwhelmed by the second day. "There is so much to absorb," she said, "but [this kind of seminar] for practitioners is a great service."

The IAB publishes the Selected Equipment List (SEL) on an annual basis to provide the emergency response community with equipment and system acquisition and operation assistance. Based on the information presented during the workshop, the ICIS subgroup has updated the SEL items that pertain to information security systems. The subgroup will also prepare a report based on discussions during the workshop that will be made available to the emergency response community. For more information visit the IAB website at http://www.iab.gov/.

Left to right: Troy Sella, Los Angeles County Sheriff's Dept.; George Bakos, ISTS Senior Security Expert; Ron Burch, Phoenix Fire Dept.; Harlan McEwen, IACP; Joey Booth, Louisiana Dept. of Public Safety.

ER3C Appoints New Fellows

This winter, the ISTS Emergency Readiness and Response Research Center (ER3C) appointed two fellows.

Klaus Christoffersen joined the ER3 Center in February and will be working on Physiological Monitoring and Mass Casualty Simulation. Christoffersen is a cognitive engineer and principal consultant of Cognizant Systems Design in Hamilton, Canada. He has conducted research and consulted for clients in a variety of domains including health care, transportation, NASA space operations, and industrial process control. His primary interests are in advanced visual displays for monitoring and problem solving in real-time applications.

Stephen P. Linder, Ph.D., joined the ER3 Center in December 2005 and will be developing methods for adaptively assessing the physiological state of personnel responding to emergencies, and developing new simulation approaches for health assessment in mass casualty events. Linder brings to the Casulty and Responder Remote Monitoring Appartus (CARRMA) project his expertise in architecture, design, and construction of intelligent machines, including biomedical systems. He received a B.S. degree in mechanical engineering from the Massachusetts Institute of Technology in 1982, and a M.S. in computer systems engineering and a Ph.D. in electrical and computer systems engineering from Northeastern University in 1996 and 1998, respectively. He was previously with the Applied Research Laboratory, Pennsylvania State University working on target tracking and sensor data fusion, and a faculty member in computer science at the State University of New York, Plattsburgh. While at Dartmouth he has been a faculty member in computer science teaching courses in robotics, software design, and computer graphics.

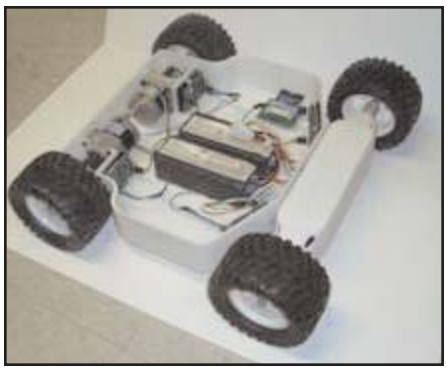
Automated Assistance for Disaster Response (AADR)

Exploring collapsed buildings, sites of industrial accidents, natural disaster areas, and battle zones is dangerous and difficult. Researchers Laura Ray, associate professor at the Dartmouth Thayer School of Engineering, and Devin Balkcom, assistant professor of computer science, are building sensors and robots to help with these risky endeavors. Their tools are aimed at increasing rescuers' situational awareness, allowing the rescuers to work more effectively with less risk.

Sensor technology, including cameras, microphones, gas, and sensors, can expand an emergency responder's awareness; these resources help locate victims or warn of dangerous situations. One key challenge is getting the sensors into the most relevant areas. Mobile robots provide one approach; robots may be able to squeeze into tight areas, and are somewhat expendable. The Ray/Balkcom team is designing and building relatively inexpensive mobile robots that can be used for sensor delivery. During the summer of 2005, they deployed a solar powered robot at Summit Greenland for field testing and evaluation of power system control. Not only should the robots have a reliable power system, they also need to be, well, mobile.

"Even the best-designed robots get stuck. If a car gets stuck in snow or sand, a skillful human driver might be able to free it using clever steering or dynamic rocking", says Balkcom. "When NASA's Opportunity robot became stuck in Martian sand in May, 2005, skillful human drivers were more than 50 million miles and a six-minute speed-of-light communication delay away."

A better understanding of non-traditional locomotion strategies may allow mobile robots to become more capable without redesign, explains Balkcom. To study this, he and Thayer School students Nelson Rosa, Jr. and Joshua Pyke have built an experimental testbed: a sandbox with a computer-controlled car (a.k.a. robot). This group has found the right series of programmed rocking motions that allow the car to free its wheels buried in sand. In future work, the team will explore more complicated motions, such as using the wheels like fingers to dig and shape the terrain to allow better mobility.



Four-wheel-drive robot prototype

Mobile robots are not the only focus of Balkcom and Ray's work into safely exploring hazard environments. Suppose a large building has fallen, leaving an unstable mountain of rubble.

"If you've played Jenga, you know how hard it can be to guess if the pile is about to collapse", says Balkcom.

Balkcom and graduate student Anne Loomis are exploring automated reasoning to understand stability. They have observed that computing the stability of a pile of objects can be done much more efficiently if something is known about the stability of a portion of the pile. This observation allows quick computation of sequences that a pile may be safely taken apart. The ultimate goal? Wearable sensors and displays that warn rescuers of physically unsafe situations, and give advice about how to safely extricate a victim from a rubble pile or safely cross unstable terrain.

For more information, visit http://www.cs.dartmouth.edu/~robotics

ISTS Researcher Assists with Katrina Relief Efforts

by Jenny Bodwell

The feeling as you walk down the nearly empty streets of East Biloxi, Mississippi, is one of utter devastation; an anthill trodden by an unheeding foot, just barely beginning to rebuild its home. East Biloxi is situated on a peninsula. With water on three sides, it was one of the hardest hit areas on the Gulf Coast, and one of many other disaster areas totally forgotten while the media continues its focus on "Nawlins," as it's pronounced in Mississippi.

Along with eight other staff members and around 35 Dartmouth students, I volunteered my time for two weeks, December 8-21, working with an organization, Hands On USA (HOUSA), which has been instrumental in helping the City of Biloxi get back on its feet. If you have ever doubted that a small group of caring people can accomplish a great deal, one day with these people will change your views forever. Although most of the downed trees had been taken care of, there was still plenty of work to keep the tree crew busy while I was there. Other jobs that people worked on were gutting the interiors of houses, demolding the gutted houses, tarping roofs, helping at the Humane Society, helping at the Salvation Army warehouse, helping on the SA canteen trucks that were still serving hot meals to hundreds of people, and putting up plastic street signs so that navigation was once again possible.

Biloxi was very lucky in that it has HOUSA to help with its recovery efforts. Many other local communities are not as lucky, so HOUSA volunteers go to neighboring towns on a fairly regular basis. Despite the 1,000 + volunteers and over a million dollars in labor that HOUSA alone has donated to the community, they are still a long way from recovery.

Jose, Jenny Bodwell and Zach (also from NH)

This experience gave me a whole new perspective on my work at ISTS in the ER3C, where I help create training simulations for first responders. Not only is there a great need, there is still a great deal to be done.

Link to pictures:
http://public.fotki.com/biloxitrip/

Link to my website (stories):
http://people.ists.dartmouth.edu/~jbodwell/biloxitrip.html.

ISTS Researcher Highlight

Laura E. Ray, Ph.D.

An Associate Professor of Engineering, she received her B.S.E., summa cum laude, and her Ph.D., in mechanical and aerospace engineering, from Princeton University. She received her M.S.E. from Stanford University, winning first prize in the Lincoln National Design Competition for her master's project. The recipient of numerous fellowships and awards, she was a faculty member at Clemson University and Christian Brothers University before joining Dartmouth's Thayer School in 1996. At Thayer School she teaches courses in control theory, dynamics, and computer-aided design and analysis.

What are your primary research interests?

Dynamics and controls is my broad area of research. Within that I have three sub areas/applications: 1) mobile robots; 2) active noise control; and 3) non-destructive evaluation – methods of inspecting structures for damage. We are looking at ways to do that to provide additional information about the health of the structure besides just the presence or absence of damage.

What are you working on at ISTS?

I am working on Automated Assistance for Disaster Response (AADR) at ISTS along with Devin Balkcom. The goal of our project is to build robots for disaster response teams. We are exploring solutions to two key problems: sensor delivery, and automated physical reasoning about disaster situations. **(see article, page 3)**

How did you decide to become an engineer?

The real reason is kind of funny – when I was 10 years old some mean boys had thrown my sister's bicycle off a bridge. I retrieved the bicycle, and it was mangled. Feeling bad about what happened, I decided to fix it. This couldn't be done of course without my taking the bicycle apart. I took it apart down to the bearings. It was a great way to spend the summer, and I was hooked at that point, even though I had never heard of engineering.

When I was in college, at Princeton, I had to choose between mechanical and electrical engineering. I chose electrical engineering at first, but I felt like I was missing out on opportunities in other engineering departments. My faculty advisor explained to me that I could choose an engineering discipline and not be tied to it for the rest of my life. I changed my major to mechanical and aerospace engineering. This put me into the world of mechatronics thus allowing me to keep one foot on both sides of the fence: one side being mechanical and the other electrical. The research side of what I do with robots involves both disciplines.

The engineering dean at Princeton once told me, "If you broadly educate at the undergraduate level you can prepare yourself for lots of different jobs." This has held true.

What professional accomplishment are you most proud of?

At this point I have to say that taking something from the pages of a journal to practice has been most rewarding. A couple of years ago two of my colleagues and I started a company called Sound Innovations. We are commercializing active noise control algorithms for hearing protection. This was originally a Ph.D. project involving signal processing and adaptive control. Our company is developing products to provide more effective protection against noise-induced hearing loss. You don't always see what you are doing in the research laboratory put into practice. It will be very exciting when the first product goes out the door.

What are your favorite non-work activities?

I have four children – that's my 'non-work' activity in a nutshell! In the summer I have more time to relax and to go biking and camping with my kids. If there were snow this winter we would be out cross-country skiing.

What was the last book you read?

I'm just finishing up *Garbage Land: On The Secret Trail of Trash* by Elizabeth Royte. She lives in NYC and decided to follow the trail of her garbage. She got into the trucks with her sanitation men and followed the garage trail to the end. She visited landfills, sewage plants, trash incinerators, and composting and recycling operations. At the end of the book you wonder whether it is possible to get down to zero garbage. It's a good book!

What do you most like about Hanover or Dartmouth?

I guess what I like most about Dartmouth are the people, the students, and the colleagues that I work with. Dartmouth places value in collaboration and partnerships. There are many opportunities at Dartmouth and in Hanover for collaborative research. As a beginning investigator ten years ago I could not have envisioned the diversity of activities that I am part of today.

What I like most about Hanover is that it is a nice community. Hanover is safe and a good place to raise children, which makes the winters bearable.

What do you think is the best kept secret about Dartmouth?

I don't know that Dartmouth has any secrets! Have you ever heard of Geocaching? Geocaching is somewhat like the regional Valley Quests a place-based education program that uses treasure hunts to celebrate community natural history, cultural sites, stories, and special places. I thought that these organized "treasure hunts" were unique to this area. Geocaching is an international activity in which caches are hidden around the world, and GPS is used to find them. There are quite a few treasures hidden on or near the College campus. We are just starting this with my 13 year old son. There are certain caches called "traveling caches". So, if you wanted your treasure to go to China, you place it in a traveling cache, provide the destination, and it might make it there over time and a series of moves from cache to cache by total strangers. Geocaching (http://www.geocaching.com/) is great fun!

Tiny Trusted Third Parties

How can two millionaires learn who is the richer, without actually revealing their bank balances? *Secure Multiparty Computation* (SMC) provides a way for them to do this. SMC allows parties who do not trust each other to perform a joint computation on private data, such that each participant does not reveal their private data to anyone else. Theoreticians have developed many protocols for SMC, but they are not scalable to large computations, especially where indirect indexing is required. Some examples which are probably infeasible for existing protocols, include optimization algorithms on large datasets, like dynamic programming and Dijkstra's algorithm for graph shortest paths.

Trusted Third Parties to the Rescue

ISTS Researchers, Sean Smith and Alexander Iliev are developing scalable solutions for SMC using small trustworthy devices, or Trusted Third Parties (TTP): the participants send their inputs to a TTP, which computes the answer and sends it back to each participant.

Alexander Illiev, Ph.D. student

Why should stakeholders trust this TTP, especially if it is not in their control? According to the ISTS team, the TTP is specifically built for this purpose—it is physically armored against attempts to observe or modify its computation, and has an infrastructure to prove itself and its output to remote parties (akin to remote attestation in the Trusted Computing Group (TCG) terminology). The device they are using, which Smith helped build, is the IBM 4758 secure coprocessor.

Their current work focuses on the issues of cost and storage capacity: the 4758 costs about $2500, and has very little internal secure memory, which necessitates the use of external untrusted memory and expensive algorithms to do so securely

They hypothesize that the performance problems of SMC on the 4758 can be solved by a new hardware design focused and optimized on a class of operations which dominate the secure paging algorithms. These algorithms need very little secure space, so the new device will be very small: a Tiny TTP. They hope this can reduce the cost of the device.

"Using Tiny Trusted Third Parties is squarely in the spirit of minimizing the Trusted Computing Base," says Smith. "Our desired outcome is that the Tiny TTP is fast enough for large computations that people and organizations want to do, and is cheap enough that it will actually be used."

The group is currently prototyping the SMC system on the 4758 (without SMC-specific hardware optimizations). Shortly they will begin transferring it to an optimized hardware implementation on an FPGA (Field-Programmable Gate Array). They predict the FPGA implementation should provide two to three orders of magnitude performance increase.

For more information, visit http://www.cs.dartmouth.edu/~sasho/tttp/

Invited Speakers Winter 2005-06

January 9, 2006
Dr. Christian Skalka
University of Vermont.
"Logic and Practice of Risk Management"

February 22, 2006
Phil Venables
Managing Director and Chief Information Risk Officer Goldman Sachs Group.
"The Resilient Enterprise: Convergence of Technology, Security, Redundancy and Risk"

February 24, 2006
Dr. Kirk Shelley
Associate Professor, Department of Anesthesia at Yale University School of Medicine.
"Analysis of the Photoplethysmographic Waveform: Designing the 3rd Generation of Pulse Oximeters"

January 25, 2006
Dr. Klaus Christoffersen
Principal consultant of Cognizant Systems Design in Hamilton, Canada.
"Cognitive Engineering: Design for Cognitive Performance"

February 23, 2006
Dr. Ian Brown
University College London and Cambridge-MIT Institute.
"The Dark Side of the (ubiquitous computing) Force"

For our latest events news, visit our website at http://www.ists.dartmouth.edu/events.php

ISTS Institute for Security Technology Studies at Dartmouth College Quarterly

Institute for Security Technology Studies at Dartmouth
(Interdisciplinary research and education for cyber security and emergency response technology)
45 Lyme Road
Hanover, NH 03755-1219
phone: (603) 646-0700
fax: (603) 646-0660
email: info@ists.dartmouth.edu
www.ists.dartmouth.edu

Kudos

Susan McGrath, Director, Emergency Readiness and Response Research Center at ISTS and associate professor of engineering and lecturer at the Thayer School of Engineering, was recently appointed to the Personal Protective Equipment Committee at the Institute of Medicine, (IOM - part of the National Academies). The committee will examine scientific and technical issues in the development and use of personal protective equipment and explore emerging research areas. McGrath was also asked to join the Emergency Management Technical Committee, part of the Organization for the Advancement of Structured Information Standards (OASIS), where she will assist in the development of standards for emergency response data exchange and interoperability. McGrath's research interests include mobile computing and intelligent software applications for biomedical, emergency management, and command and control applications.

Visit our ISTS on-line publication library at http://www.ists.dartmouth.edu/library and subscribe to *ists-papers* for new ISTS publications.

Recently added publications:

S Lyu and H Farid, *"Steganalysis Using Higher-Order Image Statistics"*, IEEE Transactions on Information Forensics and Security, Vol. 1, No. 1, March 2006
http://www.ists.dartmouth.edu/library/179.pdf

K Minami and David Kotz, *"Scalability in a Secure Distributed Proof System"*, Proceedings of the Fourth International Conference on Pervasive Computing, May 2006
http://www.ists.dartmouth.edu/library/173.pdf

INFORMATION:
Web: www.ists.dartmouth.edu

CONTACT:
Email: info@ists.dartmouth.edu
Telephone: 603-646-0700
Fax: 603-646-0660

ISTS: *Interdisciplinary research and education for cyber security and emergency response technology.*