

From Our Director

We began the new academic year with a burst of activity and the launching of many new projects. Through a \$5 million grant from the Bureau of Justice Assistance in the Department of Justice, we began to fund nine major new projects. Those in the Cyber Security and Trust Research Center (CSTRC) focus on security, privacy, and trust in computing systems and computing media, and those in the Emergency Readiness and Response Research Center (ER3C) will develop new technologies for disaster simulation and situational awareness and help make the technologies available to emergency response organizations; more details are in this newsletter.

In addition, HSARPA recently awarded a grant to support research and development of a system for wireless network security. ISTS is proud to have Aruba Networks as its partner in this project, along with collaborators at the University of Massachusetts Lowell.

Since the last newsletter, ISTS researchers have published another seven technical papers and analytical reports, primarily in peer-reviewed academic conferences and journals. Be sure to visit the library on the ISTS web site, and subscribe to the "ists-papers" mailing list to be notified of new items as they are posted.

A special congratulations to ISTS's four new Ph.D graduates and four new M.S. graduates.

Clearly it is an exciting time here at ISTS, as we continue to deliver on our three major goals:

RESEARCH, to provide thought leadership to the nation and to the world, among academics, practitioners, and policymakers.

EDUCATION, to increase the number of students and faculty involved in security technology research, and to increase community awareness of security technology challenges and solutions.

OUTREACH, through collaborations that deploy our security technology and encourage knowledge transfer for both public and private benefit.



Photo: Joe Mehlhag '09

David Kotz

ISTS and Dartmouth part of new NSF-funded Cyber Trust Center by Susan Knapp

Five-year, \$75 million project to examine the cyber safety of the nation's power grid

Researchers with Dartmouth's Institute for Security Technology Studies (ISTS) are part of a new center that will address the challenge of how to protect the nation's power grid. The National Science Foundation has awarded \$7.5 million over five years to the project, which will be led by the University of Illinois at Urbana-Champaign, and will also involve researchers at Cornell University and Washington State University.

The new center, called Trustworthy Cyber Infrastructure for the Power Grid (TCIP), will aim to improve the way the power grid cyber-infrastructure is built and maintained, making it more secure, reliable, and safe.

"The power grid is the infrastructure that enables all other infrastructures, like banking and finance, and oil and gas," says Sean Smith, a researcher with ISTS's Cyber Security and Trust Research Center and an Assistant Professor of Computer Science. "However, the power grid's security and reliability depends on what is essentially a vast distributed computing system that spans many organizations and environments and involves thousands of employees."

Smith will lead a multi-university research team examining how to build a secure and reliable computing base. They will investigate hardware approaches to the security and reliability challenges in the grid's cyber infrastructure. This work builds on his previous Dartmouth research and on his prior experience working in industry.



Photo: Joe Mehlhag '09

Sean Smith

Other research teams will examine data collection, trustworthy information exchange, and quantitative validation. Former ISTS director David Nicol, now a professor at the University of Illinois, will lead the validation section, using tools and techniques developed in part while he was at Dartmouth.

TCIP was one of two new centers announced on August 15 by NSF, part of their 2005 Cyber Trust program. Cyber Trust, the focus of the foundation's cyber-security efforts, was designed to create a system that guarantees the reliability of computers and networks underlying the nation's infrastructures, even in the face of cyber attacks.

Inside

HSARPA funds WLAN security	2
New projects supported by Bureau of Justice Assistance	3
World's Smallest Micro Robot	5
I3P Update	5
An Intern's ISTS Experience	6

M.A.P. (Measure, Analyze, Protect): security through measurement for wireless LANs

With the rise of Voice over Wireless LAN (VoWLAN), any complete WiFi security solution must address denial of service attacks such as kicking off other clients, consuming excessive bandwidth, or spoofing access points, to the detriment of legitimate clients. Even an authorized client may be able to sufficiently disrupt service quality to make the network ineffective for legitimate clients.

We take a three-point "MAP" (measure, analyze, protect) approach to develop an integrated and extensible framework to address existing and future attacks on WiFi networks. Specifically, we focus our efforts on an integrated set of new components that allow a WiFi network operator to measure and analyze WiFi and VoWLAN activity, and in real-time to identify and defend against MAC- and IP-layer attacks on that infrastructure. Our plan includes three overlapping phases: research, prototype development, and deployment on Dartmouth's campus-wide wireless network; the third phase is an option.

Measure: we will develop novel and scalable techniques to collect multi-channel MAC-layer traces of the wireless environment, building on our wireless-measurement infrastructure. We will extend our state-of-the-art honeypot technology to build "wireless honeypots" that, when attacked and subsequently used to attack the wireless network itself, allow us a detailed look at the attacker's methods and activities. Finally, we will develop novel honeypots that emulate real VoIP handsets, in anticipation that these handsets will be the target of future attacks.

Analyze: we will explore two novel statistical methods to the real-time analysis of wireless network status and traffic, Tree-Augmented Bayesian Networks (TAN) and Principal Component Analysis (PCA). We use TAN to efficiently detect known attacks and PCA to detect anomalies caused by unknown attacks; combined, they should be able to automatically derive efficient detection models in real time with minimum human intervention.

Protect: we will develop a policy-driven protection engine that leverages existing defense mechanisms; the R&D challenge here is to integrate them into our analysis framework and to evaluate the impact of automated defenses on well-behaved users in a network.

Deployment.

With our partner, Aruba Networks, we will develop and deploy prototypes for testing in Phases 1-2, and then in optional Phase 3 we will deploy our prototypes across Dartmouth's next-generation campus-wide WiFi network; this testbed provides valuable data for the research team and valuable input into Aruba's product pipeline.

Novelty.

We plan significant, novel extensions to existing technology; these techniques have never been applied to WiFi networks, to VoWLAN applications, or at the scale necessary for large deployment. Our integrated end-to-end MAP approach is new, and our proposed campus-wide deployment is unprecedented in scope and scale.

Our MAP approach provides a new foundation for wireless network security, able to dynamically measure, analyze and protect a WiFi network against existing and novel threats, including rogue clients and access points, with a focus on VoWLAN use cases.

Principal Investigators:

David Kotz, Professor

Andrew Campbell, Associate Professor

Tristan Henderson, Research Assistant Professor

Guanling Chen, Assistant Professor, UMass Lowell

An ISTS project at Dartmouth College in cooperation with UMass Lowell and Aruba Networks.



Cyber Security and Trust Research Center (CSTRC)

Technology for Trust (T4T)

Sean Smith, Denise Anthony, Jamie Ford, Fillia Makedon, Douglas McIlroy

People and organizations increasingly rely on pervasively networked computer-based systems as the medium for accessing information, conducting transactions and exchanges, and communicating private information. Consumers, businesses, government officials and technologists demand "trusted" systems to ensure the safe, reliable and successful use of these systems.

Sociologists recognize that trust in these systems depends on more than simply the technology enabling them, but also on the characteristics and abilities of the actors using the systems, the context and nature of the interaction, and the (non-technical) assurance mechanisms that facilitate confidence in these systems of exchange and communication.

This interdisciplinary project will address fundamental questions about the role of different types and sources of information for establishing trust in exchange. Exploring different sources of trust, as well as different types of signals of those sources, are important for advancing our understanding of trust as an important social mechanism facilitating interaction and exchange.

This study of trust also has important real-world implications for e-commerce and exchange of information over the Internet, including if and how government policy should regulate Internet transactions, and how technology can be designed or implemented in ways that are both secure and usable.

Digital Living: Understanding PLACE

Privacy in Location-Aware Computing Environments

David Kotz, Denise Anthony, Andrew Campbell, Tristan Henderson

Digital technology plays an increasing role in everyday life, and this trend is only accelerating. Consider daily life five years from now, in 2010: we will each be surrounded by far more digital devices, mediating far more activities in our work, home, and play; the boundary between cyberspace and physical space will fade as sensors and actuators allow computers to be aware of, and control, the physical environment; and the devices in our life become increasingly (and often invisibly) interconnected with each other and with the Internet. Today, typical home users struggle to maintain the security of their home computer, and have difficulty managing their privacy online. Tomorrow, these challenges may become unimaginably complex. This 18-month project studies, and begins to address, the security and privacy challenges involved in developing this world of Digital Living in 2010.

Specifically, this project focuses on the advent of sensor networks, and their applications in the home and work environment. Although sensor networks have been an active area of academic research, and are commercially available for deployment in industrial settings, sensor networks will soon have many uses in enterprise and residential settings. People will live in spaces, or work with devices, that have embedded sensing capability. For people to accept this new technology into their lives, they must be able to have confidence that the systems work as expected, and do not pose unreasonable threats to personal privacy.

This confidence results from a variety of technical and organizational mechanisms. This project delves into the sociological underpinnings of privacy and trust in digital living, into the technological foundations for secure and robust sensor networks, and into mechanisms for users to express control over information about their activity.

Digital Image Forensics (DIF)

Hany Farid

It is probably fair to say that it is no longer true that seeing is believing. The ease with which digital media can and is being manipulated and altered is simply stunning. At least one consequence of this trend is that audio, image, and video recordings no longer hold the unique stature as a definitive recording of events. And, while the technology to alter digital media is developing at break-neck speeds, the technology to contend with the ramifications is lagging seriously behind. There is, therefore, a critical need to develop tools to detect tampering in digital media.

Statistical tools to detect various forms of digital tampering will be developed to determine if an image has been altered from the time of its recording. These approaches work on the assumption that although tampering may leave no visual clues, it may, nevertheless, alter the underlying statistics of an image.

Integrating Self-Awareness and Self-Healing Systems (SASH)

George Cybenko

This project will apply Process Query System technology, successfully developed in part by previous DHS funding at ISTS, to the important emerging area of autonomic systems and computing. The goal is to develop a software framework and implementation that will simplify the operation of complex computing systems, such as server farms and critical infrastructure information technology, as well as making such systems more robust with respect to cyber attacks and organic failures and degradations. This work will establish and enhance regional expertise in autonomic systems development.

Emergency Readiness and Response Research Center (ER3C)

Casualty and Responder Remote Monitoring Apparatus (CARRMA)

Susan McGrath, George Blike

The goal of this research is to protect responders and improve casualty triage and treatment by providing decision makers (such as EMTs, scene commanders, and definitive care sites) with accurate and timely information regarding the physiological state and location of monitored individuals. The project will entail: collection and analysis of data from physiological sensors in clinical and field environments; design, implementation and testing of various physiological models and health state classification algorithms; and development of an embedded processor-based hardware platform to collect and distribute data.

Communications, Applications, and Network Development for Emergency Response (CANDER)

Susan McGrath, Andrew Campbell, David Kotz, Daniela Rus

The goal of this research is to improve emergency response situational awareness by providing decision makers (such as EMTs, scene commanders, and definitive care sites) with accurate and timely information regarding the environment and state of responders on the scene of a high consequence event. The Communications, Applications, and Network Development project will investigate wireless communications mechanisms to ensure reliable and prioritized information flow between event sites, command and control locations, and definitive care sites and applications for situational awareness at definitive care sites. This research program will contribute to the knowledge base in embedded systems development, wireless networking, sensor networks, clinical and emergency medicine, mobile computing and human-computer interface scientific communities.

Simulation of Large Scale Catastrophic Events (SLSCE)

Dennis McGrath, Joseph Rosen

Natural and man-made catastrophes overwhelm the emergency response resources of the communities where they strike. Whether the result of industrial accidents, terrorist attacks, or natural disasters, large numbers of casualties may result. An effective response to catastrophic events requires that personnel at all levels of command, including community first responders, hospital personnel, state, federal, and private-sector participants, must be appropriately prepared. Simulations with responders in-the-loop provides a safe environment for rehearsing response plans and evaluating new technologies for incident command.

This project seeks to develop synthetic environments that approximate the effects of catastrophic events (biological, nuclear, chemical), as well as the resources that emergency responders at all levels would apply in response to these events. The research will build on previous work in synthetic environment research for emergency response at ISTS. Models, data, and simulation frameworks (including game engines) will be employed to build multi-resolution simulations of catastrophic scenarios. By working with local and regional emergency response organizations, we will create data driven simulations that realistically represent the capabilities and limitations of catastrophic event responders.

Automated Assistance for Disaster Response (AADR)

Devin Balkcom, Laura Ray

The goal of the project is to provide robotic machines that disaster-response teams find useful. Exploring collapsed buildings, sites of industrial accidents, natural-disaster areas, and battle zones is dangerous and difficult. Machines should increase rescuers' situational awareness, allowing them to work more effectively with less risk. Balkcom and Ray are exploring solutions to two key problems: sensor delivery, and automated physical reasoning about disaster situations.

Sensor technology, including cameras, microphones, gas sensors, and heat sensors, can expand a responder's awareness, helping to locate victims or warning of dangerous situations. The primary challenge is delivering the sensors to the most relevant area. Mobile robots provide one approach; robots may be able to squeeze into tight areas, and are somewhat expendable. However, even the best-designed robots get stuck when the unexpected happens. The primary focus of the current work on sensor delivery is in freeing stuck vehicles using clever steering or dynamic rocking.

Such non-traditional locomotion strategies are used by human drivers when a car is stuck in snow or sand, and a better understanding of these strategies may allow mobile robots to become more capable without redesign. Even if no survivors are found, search teams are exposed to great physical risks. One of the most common risks is unstable piles of rubble. Balkcom and Ray are exploring the problem of automated reasoning about stability. If the current exploratory work is successful, future projects might include such technologies as "magic" glasses that can warn the wearer of dangerously unstable blocks that should not be moved or walked on.

Translational Studies for Emergency Response (TRANSFER)

Susan McGrath

The success of ER3C research depends largely on involvement of domain experts from the emergency response community and technology development specifically intended to facilitate transition of ER3C products to the community it serves. This project will bring together researchers, emergency responders and technology transfer experts to organize feasibility studies (e.g., exercises and field tests) to provide feedback on the research agenda of each focus area. We target specific resources to further development of research products to promote transition of technologies to the emergency response community. This is a continuation of the ER3C approach to technology transfer: in 2005 ER3C supported the City of Lebanon in performing virtual mass casualty exercises for the Upper Valley, and plans to work with Port Authority or NY/NJ and Fort Monmouth on emergency response scenarios for New York City.

ISTS researchers build world's smallest mobile robot

by Susan Knapp

In a world where "supersize" has entered the lexicon, there are some things getting smaller, like cell phones and laptops. Dartmouth researchers have contributed to the miniaturizing trend by creating the world's smallest untethered, controllable robot. Their extremely tiny machine is about as wide as a strand of human hair, and half the length of the period at the end of this sentence. About 200 of these could march in a line across the top of a plain M&M.

The researchers, led by Bruce Donald, the Joan P. and Edward J. Foley Jr. 1933 Professor of Computer Science at Dartmouth, report their creation in a paper that will be presented at the 12th International Symposium of Robotics Research in October in San Francisco, which is sponsored by the International Federation of Robotics Research. A longer, more detailed paper about this microrobot will also appear in a forthcoming issue of the Journal of Microelectromechanical Systems, a publication of the IEEE, the Institute of Electrical and Electronics Engineers.

"It's tens of times smaller in length, and thousands of times smaller in mass than previous untethered microrobots that are controllable," says Donald.

"When we say 'controllable,' it means it's like a car; you can steer it anywhere on a flat surface, and drive it wherever you want to go. It doesn't drive on wheels, but crawls like a silicon inchworm, making tens of thousands of 10-nanometer steps every second. It turns by putting a silicon 'foot' out and pivoting like a motorcyclist skidding around a tight turn."

The future applications for micro-electromechanical systems, or MEMS, include ensuring information security, such as assisting with network authentication and authorization; inspecting and making repairs to an integrated circuit; exploring hazardous environments, perhaps after a hazardous chemical explosion; or involving biotechnology, say to manipulate cells or tissues.

Donald worked with Christopher Levey, Assistant Professor of Engineering and the Director of the Microengineering Laboratory at Dartmouth's Thayer School of Engineering, Dartmouth Ph.D. students Craig McGray and Igor Paprotny, and Daniela Rus, Associate Professor of Electrical Engineering and Computer Science at the Massachusetts Institute of Technology.

Their paper describes a machine that measures 60 micrometers by 250 micrometers (one micrometer is one thousandth of a millimeter). It integrates power delivery, locomotion, communication, and a controllable steering system - the combination of which has never been achieved before in a machine this small. Donald explains that this discovery ushers in a new generation of even tinier microrobots.



Bruce Donald and Igor Paprotny display models of their microrobot that are 1,000 times their actual size. To illustrate how small these machines are, the white disk represents a cross section of a human hair.

continued on page 6

I3P Institute for Information Infrastructure Protection

Update on the I3P Knowledge Base

by Patricia Erwin

Over the past year the Institute for Information Infrastructure Protection (I3P), a consortium of leading national cyber security institutions, has increased its membership, initiated two major multi-year research projects, and embarked on a planning process that will take the Consortium beyond 2007. A central program of the I3P is the development of the I3P Knowledge Base. The Knowledge Base has two distinct functions; it is the official web-site presence for the Consortium, and as such has stretched and grown to reflect information needs generated by organizational changes.

New Consortium initiatives have helped refine and focus the role of the I3P Knowledge Base in serving as the online voice of the Consortium. To better promote an awareness of our members' activities, I3P Consortium News was recently added to the public area of the Knowledge Base. This service highlights significant awards, events, and news from our members.

The public side of the I3P Knowledge Base serves as a digital commons of web-based tools and services. The I3P digital commons presently provides access to funding opportunities in relevant research areas, a calendar of cyber security events, and I3P Security in the News - a highly valued daily cyber security news aggregation service. Prior to February 2005 this was the

focus of much of our development work. A new publicly available feature of the Knowledge Base is the Cyber Security Directory. This directory is a searchable international listing of organizations with a focus on cyber security.

Over the next year the I3P will integrate the publicly available cyber security digital library into the commons. The value of the I3P digital library is to provide quick access, in one comprehensive index, to the resources available in the broad areas of information infrastructure protection and cyber security. Some of this information has never been made available to the larger research community, and as such falls into the category of 'grey literature.' As the I3P dedicates increasing effort and resources to actively coordinating and funding cyber security research, a variety of unique information resources will be produced, including literature searches, technical bulletins, and research results not generally available elsewhere.

The I3P Digital Library will be available to the public in early 2006.

For a complete list of tools and services available via the I3P Knowledge Base, please see [Overview of the Knowledge Base](https://www.thei3p.org/about/kboverview.html) [https://www.thei3p.org/about/kboverview.html].

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

Robot - continued from page 5

McGray, who earned a Ph.D. in Computer Science working on this project in Donald's lab, adds, "Machines this small tend to stick to everything they touch, the way the sand sticks to your feet after a day at the beach. So we built these microrobots without any wheels or hinged joints, which must slide smoothly on their bearings. Instead, these robots move by bending their bodies like caterpillars. At very small scales, this machine is surprisingly fast." McGray is currently a researcher at the National Institute of Standards and Technology in Gaithersburg, Maryland.

The prototype is steerable and untethered, meaning that it can move freely on a surface without the wires or rails that constrained the motion of previously developed microrobots. Donald explains that this is the smallest robot that transduces force, is untethered, and is engaged in its own locomotion. The robot contains two independent microactuators, one for forward motion and one for turning. It's not pre-programmed to move; it is teleoperated, powered by the grid of electrodes it walks on. The charge in the electrodes not only provides power, it also supplies the robot's instructions that allow it to move freely over the electrodes, unattached to them.

The work was funded in part by the Department of Homeland Security, Science and Technology Directorate, through ISTS.

Dartmouth Student Shares ISTS Experience



Jessica Glago

Since January I have interned for the Distributed Honeypots Project at ISTS through the Women in Science Project (WISP) at Dartmouth. The Honeypots project is designed to set up virtual computers to attract hackers and learn about their behavior through observation. A large amount of data is being collected, which then must be sorted and analyzed by our team. The majority of my time has been spent fixing small

bugs and adding small utilities to the program we use to view the data. The sheer volume of the data collected can be overwhelming, and is also difficult for an analyzer to try to explain to an outsider. To make it easier, I have been working on ways to display some key statistics about the collected data by using a PHP (web scripting language) graphing library. My goal is to enable individuals to get a feel for hacker behavior patterns without having to be specifically familiar with the methods employed. Although being suddenly immersed in this world of technobabble was initially quite daunting, I could not have been surrounded by more nice, patient, and helpful people. Whenever I was confused by the jargon, my coworkers made sure to take the time to translate for me. In training for my internship, I also took a computer security class offered by the Thayer School of Engineering. Between the classroom instruction and exposure to real world experiences, I feel that I have learned a great deal as a result of the help they have given me. I look forward to continuing to learn, and hopefully contribute, through this valuable and fun internship.

- Jessica Glago '08