

From Our Director

In this issue we are proud to highlight eight new projects we're launching this fall. Through funding from NIST we are able to expand our existing programs in emergency readiness and response, in which we develop technology for automating triage in large-scale disaster response, simulation technology for exercising groups of first responders, and robots for emergency response. In cyber security and trust, we are launching a major new program in scalable, secure sensor systems, which have broad applications in homeland security and beyond, and a seed project to investigate cyber security challenges in the financial sector. With support from the Bureau of Justice Assistance (in the Department of Justice) we have just funded three new seed projects: to develop robots for support in incidents involving hazardous materials, to explore miniature chemical/biological sensors of unprecedented selectivity and sensitivity (using nanocapacitive techniques combined with molecular imprinting), and to develop software that can derive "fingerprints" for various Wi-Fi network cards.

ISTS is also proud to be involved in several outreach projects. In this issue we highlight one of our Fellows, Apu Kapadia, who worked with grade-school children in Dartmouth's summer robotics camp, and Professor Denise Anthony's work with the federal cyber exercise (Cyber Storm) earlier this year.

Finally, ISTS is coordinating a group of other centers on campus this year to sponsor a series of events focused on "Freedom and Technology," a fascinating interdisciplinary theme that touches on issues of broad importance in our world today.



David Kotz

Photo: Joe Miehl '09

Summer Robotics Program

ISTS Fellow Apu Kapadia participated in this year's Summer Robotics Program for Upper Valley youth, which was sponsored by the Office of the Provost and the Department of Computer Science and took place over the course of four weeks in July. One of six instructors from computer science, engineering, and physics, Apu assisted with the integration of security concepts into the robot challenges and spoke on the importance of considering security in the design process. For example, aspects of code breaking were included in the context of an archaeological mission within an ancient Egyptian tomb.

Participants had to "decipher" ancient hieroglyphic text, which influenced their robot's design for subsequent challenges. As suggested by program director Suzanne Thompson, he also stressed the importance of ethics, since identifying security vulnerabilities in the design process involves putting oneself in the "bad guy's" shoes. Apu was also a programming instructor in three of the four camps and taught the participants how to program their LEGO NXT and VexLABS Vex robots to tackle the various challenges in each camp.

ISTS recognizes the potential for robotics in homeland security and the importance of cybersecurity, and the critical need to develop future scientists and engineers in these fields. ISTS is proud to have supported this program through Apu's participation.

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



ISTS Fellow Apu Kapadia

Photo: Devin Brande

Inside

| | |
|--------------------------------|------------------|
| Organizing for Security | page 2 |
| New Research Projects | pages 2, 3 and 4 |
| Does Technology Make Us Freer? | page 5 |
| New Publications | page 6 |
| Welcome New I3P Fellow | page 6 |

ORGANIZING FOR SECURITY

Center for Digital Strategies, Tuck School of Business

How are companies organizing for better information security? How are they embedding security risk management into the extended enterprise?

In today's outsourced enterprises, effective risk management is quickly becoming a source of competitive advantage. With customers and business partners demanding greater levels of security, the security discussion is moving beyond the IT group into the business strategy units. CEOs, CIOs, and CISOs are working together to manage information security risks without inhibiting the business.

"Embedding Information Security Risk Management into the Extended Enterprise"—a report published earlier this year by the Tuck School's Center for Digital Strategies (CDS) and the Institute for Information Infrastructure Protection (I3P)—outlines the following imperatives for enabling security transformation:

Metrics: Organizations must develop simple tools to measure the benefits of cyber security enhancements that are both easy to understand and are clearly linked to the business. While traditional scorecard metrics are useful, a few composite metrics that can be shared across organizations and industries will lead to better decision making.

Investment strategies: Due to globalization and outsourcing, the flow of information within and between firms is increasing. Protecting intellectual property in this environment, particularly in organizations where information resides with multiple divisions and partners, requires a change in security thinking from a technology to a behavior focus. Organizations must get their business units around the world to take ownership of their security risks.

Culture: Senior executives must change their security posture from being reactive to proactive. Building a secure culture requires a sustained effort to inculcate the entire organization. Focused education is helpful, but an ongoing discussion around security must come from the top and engage middle management. By aligning security initiatives with the company's strategic goals, senior executives can help business partners understand the risk and business case for security as an integrated part of the extended enterprise.

The report summarizes the findings from a workshop co-sponsored by CDS and I3P, in which senior security executives from Fortune 500 firms—including 3M, Bank of America, BP, Cisco Systems, Colgate, Dell, Dow Chemical, IBM, Staples, Time Warner Cable, and the U.S. Army—debated the challenges of organizing for security and to develop an action plan for the next 12 - 18 months. To learn more about the workshop and to read the complete report, visit www.tuck.dartmouth.edu/digital-strategies, under Corporate Events.

NEW RESEARCH PROJECTS SUPPORTED BY
BUREAU OF JUSTICE ASSISTANCE (BJA)

Hybrid Sensors for Low-Level Threat Detection (HYSENS)

Joe BelBruno, Ursula Gibson

This project involves the production of prototype sensors for detection of chemical threats suitable for incorporation in an agile reporting network. Molecular recognition polymers will be used as the active element for specific detection of threats on an electronic sensor backbone. Such sensors offer protection to both to civilians and emergency first responders.

HazBot: Development of a Telemanipulator Robot with Haptics for Emergency Response

Joseph Rosen

The HazBot project ("Hazardous Materials" and "Robot") is developing a teleoperated manipulator robot capable of handling hazardous-materials events. Teleoperated manipulator robots are enabling and lifesaving tools for HazMat response. They can reach areas inaccessible to humans, and perform missions too dangerous or expensive for humans to reasonably attempt. Unfortunately, their usefulness is limited by the difficulty of controlling remote manipulators. The team plans to implement a new control device that will simultaneously simplify manipulator control and provide haptic feedback to give the operator a sense of touch via the robot. They will also develop a training simulator system to allow responders to conveniently learn and practice HazBot operation.

Behavioral fingerprinting of wireless devices

Sergey Bratus

It is possible to observe the response of an 802.11 wireless device to certain protocol events, and select behavior unique to a particular combination of hardware, firmware and software as its "fingerprint." The goal of this project is to study methods for active and other forms of behavioral fingerprinting of 802.11 wireless devices, investigate security implications of fingerprintable behaviors, and provide recommendations for detecting and counteracting fingerprinting activity.

Emergency Readiness and Response Research Center (ER3C)

Automated Remote Triage and Emergency Information Management System

Susan McGrath, George Blike, Jay Buckley

Mass casualty events, such as Hurricane Katrina, demonstrate the critical need for improved medical monitoring, assessment, and tracking technologies. The Automated Remote Triage and Emergency Management Information System (ARTEMIS) project seeks to address this need through research, development and field-testing of technologies to enhance situational awareness of medical decision makers such as EMTs, scene commanders, definitive care sites. The ARTEMIS project focuses on protecting responders and improving patient care by providing relevant and timely information regarding the physiological state and location of monitored individuals. ARTEMIS research efforts to date have produced a personal monitoring hardware platform, automated triage and sensor data processing approaches and algorithms, handheld-based applications for field medical personnel, and a prototype command and control system for event management. The proposed work will leverage prior results to address the following outstanding critical path challenges: real-time physiological sensor data processing, classification and fusion; medical models for automated complex injury and resource constrained triage protocols; and multi-tier situational awareness approaches for high-pace environments.

Simulation Architecture for Exercising Teams

Dennis McGrath

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. Simulation exercises with responders in-the-loop provides a safe environment for rehearsing response plans and evaluating new technologies for incident command.

The goal of this is 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.

Mobility Assessment for Emergency Response Robots

Devin Balkcom, Laura Ray

Robotic platforms offer the potential for increasing situational awareness through rapid emergency deployment of distributed remote sensors; augmenting navigation in urban environments; reducing hazards for human emergency responders; information gathering; and victim rescue or relief. One can envision an army of robots that used for emergency response assistance and management, expanding the capability of response coordinators and first responders to enhance situational awareness, while keeping people out of harm's way. The proposed research advances the use of semi-autonomous and autonomous mobile robots by enabling the robots to perform automated terrain diagnostics and assess mobility. Such robots could be sent ahead of manned vehicles to map "trafficability" of terrain, plan routes, and relay information back to a convoy. This information will in turn enhance the on board robot intelligence and ultimately will enable both manned and unmanned vehicles to avoid immobilization and safely negotiate off-road terrain and paved roads that may have been damaged by landslides, mudslides, and flooding.

Cyber Security and Trust Research Center (CSTRC)

Metro Sense: Scalable Secure Sensor Systems

Andrew Campbell, David Kotz, George Cybenko

Sensor networks will provide a foundation to protect and monitor our national infrastructure, including economically important businesses with global reach (e.g., stock markets), critical transport and industrial facilities, the enterprise, and the border. These tiny, low-cost wireless devices embed on-board sensing, are fully programmable, and can spontaneously form large sensor webs with thousands of distributed sensor devices. In this project, we will study, analyze, propose, deploy, and evaluate MetroSense, a radically different scalable secure sensor architecture and system capable of reliable real-time monitoring and data fusion for large-scale critical infrastructure, resources, and assets. MetroSense opportunistically leverages mobile sensors when available to deal with sparse coverage and communications when sensing. We plan to develop a campus-area sensing architecture based on three integrated components (sensing and communications, sensor security, and sensor fusion) and deploy the system incrementally across campus with the goal of using static and mobile sensors for reliable monitoring and data fusion of campus plant, spaces, and people flow. Results from this project will serve as a foundation for building secure sensor networks capable of monitoring large-scale critical infrastructure.



Information Risk in the Professional Services (IRIPS)

Sean Smith, M. Eric Johnson

Professional service industries operate on information. In the private sector, the financial services industry is arguably the leader in managing complex information security while providing professional services. As preparation for further work in both financial services and the healthcare sector, this exploratory project will study current security practices in the financial services industry. We will examine and catalog the technical and business pressures that guide security decisions and policies. This project will benefit financial services providers by both documenting current practices and challenges and developing directions for future research.

These projects are funded under award 60NANB6D6130 from the U.S. Department of Commerce. The statements, findings, conclusions, and recommendations are those of the investigators and do not necessarily reflect the views of the National Institute of Standards and Technology (NIST) or the U.S. Department of Commerce.

Cyber Storm National Exercise

In February 2006, the Department of Homeland Security conducted a national exercise called Cyber Storm, simulating an attack on the IT systems and infrastructure of U.S. businesses and government agencies. Complex crises like that simulated in the Cyber Storm exercise require different types of organizations to communicate and cooperate to understand, respond to, and resolve the crisis. Denise Anthony, associate professor of sociology and faculty affiliate in the Cyber Security and Trust Research Center at ISTS, examined the email communication patterns produced by the over 100 organizations participating in Cyber Storm. The goal of the research is to understand the nature and structure of communication networks to identify the linkages and patterns necessary for effective communication in the case of a real cyber attack.

According to the email communication patterns in the Cyber Storm exercise, a number of key governmental and industry actors played important roles in communicating information throughout the network. The National Cyber Security Division of the Department of Homeland Security played the most central role of all federal agencies, though a number of other DHS units, as well as other departments and agencies provided crucial conduits of information within the communication network. In addition to the federal organizations, a number of other governmental actors, including other national governments, as well as state and local government agencies, had significant levels of communication.

Two industries also played key roles in the communication network the IT services industry (including major ISPs, hardware and software vendors) and the energy industry. Given the nature of the exercise and the focus on the energy industry, organizations in the energy sector had to deal with significant IT problems and thus were communicating with others to try to address their network problems. The IT services industry, in contrast, was responding to and addressing problems that various organizations were bringing to their attention. That is, the IT services industry is typically the first point of contact when an organization has a problem with its IT, no matter whether the organization is a private firm or a government agency. Thus, the private firms in the IT Services Industry play a crucial role during a cyber attack, as both key conduits of information, and as analysts initially comprehending the extent and nature of the crisis. The central role played by the IT services industry in Cyber Storm was consistent with findings from the ISTS sponsored "Livewire" Cyber Exercise in 2003 that also showed a central role for the IT industry. According to Prof. Anthony, both exercises demonstrated the necessity of public-private cooperation during a cyber attack.

Does Technology Make Us Freer?

Freedom and technology focus of programming

The Dartmouth Centers Forum—a consortium of eight campus institutes—will address the theme of "Freedom and Technology" during the 2006-2007 academic year. The aim, according to David Kotz, director of the Institute for Security Technology Studies (ISTS), will be to examine the nexus of freedom and technology and to better understand how humanity and technology may best interact and coexist.

"I'm looking forward to this program, which helps us connect the different characteristics of technology and how it affects both personal and national freedoms," says Kotz, who is also a professor of computer science.

He explains that technology can be liberating, freeing us from physically hard and time-consuming labor and granting us access to information and knowledge. On the other hand, technology can also be imprisoning as it can be used to track our movements, spy on our private lives, and create a dependency on tools many of us do not understand.

"The Centers Forum is busy planning a series of exciting events that bring new insight into these opportunities and challenges," says Kotz.

The first event in the series is a lecture on October 19 by Dan Wallach, associate professor of computer science at Rice University in Houston, Texas, and the associate director of the National Science Foundation's ACCURATE (A Center for Correct, Usable, Reliable, Auditable, and Transparent Elections). His talk, titled "Electronic Voting: Risks and Research," will cover the timely topic of managing electronic voting systems in this era of hanging chads, questionable security, reliability, and accuracy. He will discuss how research in software engineering, distributed systems, and cryptography can and should impact the next generation of voting systems.

More information about the Dartmouth Centers Forum, can be found at www.dartmouth.edu/~centersforum.

Dartmouth Centers Forum partners are: Allwin Initiative for Corporate Citizenship, Tuck School; Dartmouth Center for the Advancement of Learning; Dickey Center for International Understanding; Ethics Institute; Institute for Security Technology Studies; Leslie Center for the Humanities; Rockefeller Center for Public Policy and the Social Sciences; and the Tucker Foundation.



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

New Publications

Visit our on-line publication library at <http://www.ists.dartmouth.edu>

H. Farid, "*Exposing Digital Forgeries in Scientific Images*", Proceedings of the 8th ACM Multimedia and Security Workshop, Geneva, Switzerland, 26-27 September 2006

<http://www.ists.dartmouth.edu/library/199.pdf>

M. Johnson and H. Farid, "*Exposing Digital Forgeries Through Chromatic Aberration*", Proceedings of the 8th ACM Multimedia and Security Workshop, Geneva, Switzerland, 26-27 September 2006

<http://www.ists.dartmouth.edu/library/201.pdf>

W. Wang and H. Farid, "*Exposing Digital Forgeries in Video by Detecting Double MPEG Compression*", Proceedings of the 8th ACM Multimedia and Security Workshop, Geneva, Switzerland, 26-27 September 2006 <http://www.ists.dartmouth.edu/library/200.pdf>

Felipe Perrone and Samuel Nelson, "*A Study of On-Off Attack Models for Wireless Ad Hoc Networks*", Proceeding of the First International Workshop on Operator-Assisted (Wireless Mesh) Community Networks 2006, Berlin, Germany, 18-19 September 2006

<http://www.ists.dartmouth.edu/library/210.pdf>

Andrew Campbell, Shane B. Eisenman, Nicholas Lane and Emiliano Miluzzo, "*PeopleCentric Urban Sensing*", Proceedings of the 2nd Annual International Wireless Internet Conference (WICON), Boston, MA, 2-5 August 2006 <http://www.ists.dartmouth.edu/library/203.pdf>

WELCOME



Nikos Triandopoulos
joins ISTS as I3P Fellow

Nikos comes to us from Brown University. His primary research areas are in information security, cryptography and algorithms. He will spend his year-long, I3P-funded postdoctoral fellowship working with Computer Science Professors Fillia Makedon and Jamie Ford on algorithms for high assurance in cyber-security.

INFORMATION:

Web: www.ists.dartmouth.edu

CONTACT:

Email: info@ists.dartmouth.edu

Telephone: 603-646-0700

Fax: 603-646-0660