Emergency response technology developed at ISTS was recently on display as researchers from ER3C participated in the federal demonstration area at the 7th Annual “Technologies for Critical Incident Preparedness” Conference in San Diego. The three-day conference, held this year from Oct. 31 to Nov. 2, brought together representatives from the emergency response community, government, academia, and industry to share ideas on new technology solutions for the challenges of emergency response.

Among the ISTS technologies demonstrated at the conference were the Automated Remote Triage and Remote Emergency Management Information System (ARTEMIS), game-based simulations including Unreal Triage and Grand Theft Ambulance, and the Immersive Simulation Environment for Exercises (ISEE).

“There was a lot of interest in our work and a recognition from the emergency responders of the value of our research,” says ISTS researcher Mark Stanovich.

Hundreds of visitors to the demonstration area, including representatives from the Department of Homeland Security and National Institute of Justice, got a chance to see first hand how ISTS research is helping shape the future of emergency response. In one demonstration that featured both ARTEMIS and Unreal Triage, users were able to have a simulated experience of a dirty bomb attack in a metropolitan area from the perspective of an emergency medical technician (EMT). As an EMT at the scene of the attack, users could locate casualties, tag them with “virtual” ARTEMIS sensors, and enter observations about the casualties on a handheld computer. On another computer screen, the observers could see the view from the incident commander’s perspective, where all of the sensor data and observable information about the casualties was displayed.

At the conference, ISTS researcher Dennis McGrath participated in a panel discussion on simulation and training for emergency responders. The panel included speakers from DHS, Lawrence Livermore National Laboratory, and the Federal Law Enforcement Training Center. McGrath spoke about his DHS-funded research project, Synthetic Environments for Emergency Response Simulation (SEERS). The panel gave him the opportunity to discuss some of the findings of SEERS research in applying both military simulation technology and game-based simulation technology to emergency response exercises. He also spoke about applications of simulation that go beyond t systems, including mission rehearsal exercises and analysis, and the need for federally funded efforts that encourage cooperation between researchers and emergency response professionals.
By Mica Tucker

A few days before Thanksgiving, Glen Weinberg '78, Vice President of Operating Platforms at Sun Microsystems, and Tim Marsland, Chief Technical Officer for the Operating Platforms Group, were at Dartmouth to kick-off a new partnership between Sun and Dartmouth's Public Key Infrastructure (PKI)/Trust Laboratory, directed by Sean Smith, an assistant professor of computer science. The PKI/Trust Lab is part of the ISTS’s Cyber Security and Trust Research Center.

The partnership encompasses both research and instruction in computer science, and it focuses on Sun's open source operating system called OpenSolaris. In addition, Smith's lab has been named a Sun Center of Excellence.

The Center of Excellence designation is given to teams investigating advanced ways of using Sun's software and technology in their research. Sun admired Dartmouth’s reputation for highly talented undergrads doing research, its educational support for graduate and undergraduate students with close faculty mentoring, the caliber and experience of the computer science faculty, and its tradition of applied research and development in computer science.

"I didn’t know how closely aligned our interests in security space really were until we met in April,” says Weinberg. “A lot of what I saw in Dartmouth’s PKI work was also going on at Sun.”

"There was a sweet spot here — a nice connection of needs and interest,” notes Smith. The PKI/Trust group at Dartmouth works to develop more secure and effective systems for university-based PKI. Public keys are essentially credentials one user can share with another to verify identity and access rights, to send encrypted communication, and to verify integrity of communication. The public key infrastructure is the system that enables this vetting to take place. PKI typically consists of client software, server software, and some way to hold private keys at both sides. Much of the research for Sun will build on previous work the PKI/Trust Lab has done on both the server side and the client side.

According to Smith, PKI is still not widely used outside of the government and financial sectors, in part because the client side of PKI is too cumbersome and because the fabric to link together different trust domains has not been created. Dartmouth’s PKI/Trust Lab focuses on developing a more seamless way to identify and authorize people who want to use network resources. Smith’s lab focuses on PKI for higher education, but shares its work with the broader open source community. It is a collaborative effort between ISTS, Dartmouth’s Computer Science Department and the Computing Services team.

The PKI/Trust team has been working on trusted computing technology, but this work requires an operating system that provides strong security assurances—and integrates those assurances with the hardware. With the release of OpenSolaris, team leaders saw an opportunity to contribute to the security development of a highly reliable and scalable operating system. Says Smith, referring to the former Dartmouth president and co-inventor of the BASIC programming language, "It’s the Kemeny tradition of Dartmouth: Let’s try it in the education community and see what happens, then send it out into the world.”

Weinberg says that Sun is committed to open source as the way operating systems will be developed going forward. And, the open source community’s response has been resoundingly positive. Sun hopes to take the advantage of Dartmouth’s expertise in security to lead the discussion among community developers and to encourage innovation.

As important as the collaboration on OpenSolaris development is Sun's support of the graduate curriculum in computer science. As part of this project, Smith will teach future programmers the fundamentals of operating systems. Smith will use OpenSolaris to develop such a curriculum for graduate students. In the past, it has been impossible to do so as software companies protect their proprietary systems.

Sun's OpenSolaris “is a highly reliable and scalable operating system,” says Glen Weinberg. “[OpenSolaris] provides a solid foundation on which to build.” Smith is excited about the opportunity to give graduate students an in-depth look at the framework of a high performance operating system, a view that most programming students don’t see.

Weinberg, a former student of Professor Thomas Kurtz, the co-creator with John Kemeny of the BASIC computing language, says “I am thrilled to be able to come back and set up this partnership between Sun and Dartmouth. I came to Dartmouth as a premed and graduated as a German major and a computer lover. Dartmouth gave me the opportunity to pursue the things I love.” For Dartmouth computing, Weinberg has returned the favor.

For more information about OpenSolaris, visit: http://www.opensolaris.org
In November, ISTS announced funding for three seed projects to Dartmouth faculty and staff who are beginning new research or education projects aligned with the broader ISTS mission of homeland security, whether developing technology or understanding the social and policy implications of security technology.

“We encouraged proposals from across the Dartmouth campus, and received 14 proposals from Thayer, DMS, Tuck, and Arts and Science,” says David Kotz, the director of ISTS. “The selection committee evaluated the proposals on their scientific and educational merit, novelty, and potential to bring new people and new ideas to ISTS.”

1.) Automated Analysis of Spam-Vectored Phishware
Project leads:
   George Bakos, Senior Security Expert, ISTS.
   Bill Stearns, Senior Research Engineer, ISTS.
   Irv Thomae, Senior Research Engineer, ISTS.

BACKGROUND: “Phishing” refers to online identity theft in which confidential information is obtained from the victim either through overt deceptions such as counterfeit emails and web pages, or through covert means such as keyloggers and other malware. The latter may be installed when a victim either opens infected spam or clicks on a misleading link. For faster detection of new phishing attacks, we plan to adapt the Windows virtual machine extensions developed in the ISTS Distributed Honeypots project to create “virtual victims,” to be deployed at dummy email addresses in a wide assortment of domains. A virtual victim can safely open any suspect message and follow its links, while recording exactly what happens. As compromised servers and fraudulent websites are detected, they will immediately be analyzed for signs of novelty and reported for rapid shutdown to organizations such as the Anti-Phishing Working Group.

2.) After-the-fact Radiation Dosimetry from Inanimate Objects
Project lead:
   Harold Swartz, M.D., Ph.D., Professor of Radiology and Physiology; Director of the Electron Paramagnetic Resonance Center for Viable Systems, Dartmouth Medical School.

BACKGROUND: In the event of a terrorist act or an accident releasing ionizing radiation, it is critical to rapidly and efficiently determine the radiation exposure experienced by individuals in the affected area. Recent research has found that long-lived radiation-induced unpaired electrons occurs in biological materials; these electrons can be measured by a technique termed electron paramagnetic resonance (EPR). In hard and/or dry tissues, such as bone or teeth, these resonances have been shown to provide accurate dosimetry at doses as low as 800 CgY using isolated teeth. It may thus be possible to use EPR in the event of a release of radiation. This approach has been applied to people exposed at places such as Hiroshima and Chernobyl even years after exposure. There is another approach, which could provide excellent sensitivity and ease of measurement and uses non-living material such as articles of clothing and other materials likely to be in the immediate vicinity at the time of radiation exposure. A variety of such materials have long-lived radiation-induced signals that are proportionate to dose. In this project we will systematically evaluate these materials for their usefulness in determining the radiation dose in the event of a terrorist act or an accident.

3.) Nano-optics for Matched Spectroscopy of Hazardous Materials
Project lead:
   Markus Testorf, Ph.D., Assistant Research Professor, Thayer School of Engineering.

BACKGROUND: There is a pressing need to develop improved optical sensors for detecting hazardous chemical and biological substances. We address this need by developing a scheme for matched spectroscopy based on nano-optics. Matched spectroscopy can be interpreted by implementing matched finite impulse response (FIR) filters for fingerprint emission or absorption spectra; that is, we detect a characteristic spectrum by cross-correlating the signal with the target spectrum by means of a custom-designed dispersive element. For this project, we plan to develop a novel implementation of matched spectroscopy based on nanoscopic metal-dielectric grating structures for constructing wavelength-sensitive devices. The metal structure forms cavities for optical waves guided by surface plasmons, which yields a distinct spectral response of the structure and allows the identification of a specific spectrum as a simple threshold operation. If successful, this project could result in compact hand-held spectrometers for fast detection of specific materials. Integrating the dispersive structures into conventional spectroscopic instruments would also allow the development of high-end devices that specifically address the needs of security applications.
This fall, Dartmouth’s Institute for Security Technology Studies (ISTS) appointed three new fellows who are working for the next year on a variety of projects. “Through the ISTS Fellows program we are able to increase the community of scholars and leaders involved in security technology research, and thus to broaden our nation’s capacity to confront the security technology challenges of the future,” said David Kotz, Executive Director of ISTS and Professor of Computer Science. “This research addresses fundamental problems that will become critical challenges in tomorrow’s world where technology is ubiquitous in the critical infrastructure of everyday life — at home, in the enterprise and in government.”

All fellows will be working on projects that fall under an initiative named T4T, or Technology for Trust.

Laura Kopczak will focus on understanding and creating trust in business relationships via technology. Through EnTISE, which stands for Enhancing Trust Through Information Sharing in the Extended Enterprise, she will work with researchers from the Department of Computer Science, the Department of Sociology and the Center for Digital Strategies at the Tuck school. Kopczak is a former Director of Research for the Stanford Global Supply Chain Management Forum. She specializes in supply chain restructuring, the role of non-product companies in the supply chain, and the interplay between e-commerce and supply chain management.

Apu Kapadia is working on a project called Digital Living: Understanding PLACE, Privacy in Location-Aware Computing Environments, and he is also working in Dartmouth’s Public Key Infrastructure/Trust Laboratory. He recently earned his Ph.D. at the University of Illinois at Urbana-Champaign. Kapadia’s research interests include security and privacy for heterogeneous systems, and the use of formal methods to reason about related problems. His work on the PLACE project delves into the sociological underpinnings and technological foundation of privacy and trust in digital living. His work in the PKI/Trust Lab examines integrating PKI with the richness of high-assurance operating systems and trusted computing hardware.

James Kitts’ work at ISTS will be dedicated to Understanding the Role of Interpersonal and Institutional Trust in Internet Exchange. This project uses experimental methods to examine how different types of information about a Web site’s security (e.g., reputation, technological, institutional) influence user behavior in online exchanges, including users’ willingness to pay for security information. Kitts, who is an Assistant Professor of Sociology at the University of Washington, will participate in the project from January through June 2006. He specializes in formal modeling and analysis of group interaction, social networks and social exchange systems, including online exchange.

**Virtual academy expands for medical incident management**

By Timothy Elliott

Dartmouth Medical School’s Interactive Media Laboratory recently won a $3 million competitive grant to train senior healthcare providers about WMD-related mass-casualty care and medical incident management. The project, which will be carried out in conjunction with the New England Center for Emergency Preparedness and TriMed Inc., stemmed directly from IML’s affiliation with the Institute for Security Technology Studies. The Department of Homeland Security (DHS) awarded the grant.

“IML and its partners will provide the training by creating the Virtual Medical Incident Management Institute,” said Dr. Joseph Henderson, director of IML. “With V-MIMI, we’ll be able to train senior medical and public health professionals to function within on-site incident management structures and maximize medical surge capacity during mass-casualty incidents.”

IML intends to develop a new “virtual tabletop” simulation capability for V-MIMI. The simulations will use isometric video game interfaces that will look familiar to people who play games like “SimCity” and “Civilization.” Trainees can visualize the medical response of an entire community to a terrorist attack. Specifically, the trainee can see the effects of the incident-management decisions he or she makes.

The design calls for individual trainees to interact with virtual “players” who represent various elements of the public safety community, other healthcare managers, and other response elements. A virtual mentor will guide the user through the experience. Various WMD attacks and a community’s medical response can be viewed from different angles and with different levels of detail. The components emphasize decisions relevant to mass-casualty care and medical surge capacity and capability. Surge capacity refers to an ability to handle large numbers of casualties; surge capability refers to an ability to meet the needs of patients with unusual or highly specialized needs.

V-MIMI will build on the existing advanced distance learning methods IML developed for its current DHS project: the Virtual Terrorism Response Academy. VTRA’s first course, “Ops-Plus for WMD Hazmat,” is designed to teach fire, police and EMS personnel about response to WMD incidents. It combines interactive, video-based components with video game-based simulations. The Chicago Fire Department tested the program in November, and IML intends to make the course available to first responders early in 2006.

To see VTRA samples, visit [http://iml.dartmouth.edu/education/pcpt/VTRA/demo.html](http://iml.dartmouth.edu/education/pcpt/VTRA/demo.html)
ER3C on the road

On November 10, 2005, researchers from the Emergency Readiness & Response Research Center supported a tabletop exercise in Wallingford, Conn., with simulation technology developed at ISTS. The technology, called the Immersive Synthetic Environment for Exercises (ISEE), was developed specifically to make tabletop exercises more realistic.

“Working with emergency responders helps us understand the challenges of their domain,” says principle investigator Dennis McGrath. “The goal of our research is to produce simulation tools that make emergency responders more effective.”

The Wallingford exercise dealt with a train derailment, which included a fire, multiple casualties, and a hazardous material release. Firefighters, emergency medical technicians, and police from Wallingford and neighboring communities collaborated for the first hour of the exercise to establish incident command, get the appropriate resources to the scene, and control the situation. In the second hour of the exercise, the emergency operation center (EOC) was established to manage evacuation and issue media releases. Participants in the EOC included the chief of police, the mayor, and representatives from the Department of Health and the Red Cross.

According to McGrath, ISEE is modeled after a class of multi-player computer game called role playing games (RPGs). In ISEE, emergency responders log into the simulation in one of several incident command roles, such as operations chief, public information officer, or incident commander. Players obtain resources such as personnel, equipment, and vehicles by requesting them from local dispatch or mutual aid, and then assign those resources to specific functions such as fire suppression, triage, or hazardous material containment. It also allows “control cell” players to control the pace of events, inject new events, and make dynamic changes to the scenario as the exercise unfolds.

The Wallingford exercise was the second emergency response exercise supported with ISEE this year. Exercises using computer simulation help emergency response organizations rehearse response plans, become compliant with the National Incident Management System, and conduct meaningful after action reviews. ISTS is currently working with state governments and private sector partners to transition ISEE technology into incident command training and exercise programs.

ISTS dabbles in policy research

The ISTS has joined forces with the Policy Research Shop (PRS) at the Nelson A. Rockefeller Center at Dartmouth College to study the area of first responder communications. Under the supervision of Professors Ronald Shaiko and Scott Carrell, three Dartmouth undergraduate students taking “Introduction to Public Policy Research” during the fall term of 2005 have conducted initial background research for a study examining these communication capabilities in New Hampshire and Vermont.

Students Nikolas Nartowicz ’07, Jaime Padgett ’07, and Adam Sigelman ’05 are working on the project, which is due to be completed in the spring of 2006. They have consulted on the project with homeland security experts in both states as well as with Sue McGrath, the ISTS Director of the Emergency Readiness & Response Research Center. “ISTS is delighted to be working with the PRS on this effort, says McGrath.” Communication interoperability is among the highest priorities of the emergency response community, and analysis of communication capabilities in New Hampshire and Vermont will be a great service to the region. This effort will also be a great opportunity for the students to gain insight into the challenging intersection of policy research and technology development. We expect the findings of the PRS study to influence the ISTS research agenda.”

The PRS (http://policyresearch.dartmouth.edu) is an initiative of the Rockefeller Center in which a select group of Dartmouth students work under the supervision of professors to provide quality, objective research on critical policy issues of interest to elected policymakers in New Hampshire and Vermont. The PRS was launched in 2004 as a co-curricular activity and is now being further supported through the new introductory course.

According to Rockefeller Center director Andrew Samwick, “The Policy Research Shop builds on a long tradition at the Rockefeller Center of bridging the gap between public policy research and civic engagement. By taking the introductory course or working in the Research Shop, students gain real life experience in public policy research, focusing on areas of concern to state governments, such as health care, education, and the environment. We are grateful to ISTS for enabling the Research Shop to expand its portfolio to include homeland security and emergency preparedness issues, as well.”

The PRS typically produces reports that are 5-15 pages in length, with opportunities for follow-up research upon request. The reports provide useful information in a clear format that can be of assistance during legislative deliberation. Student researchers examine emerging issues of concern for elected policy makers in both New Hampshire and Vermont. Topics are selected through a consultative process with policy stakeholders in both states.
Fall Speaker Series 2005

ISTS hosted the following four speakers this fall 2005.

**September 8, 2005**
"Wireless Internet Information System for Medical Response in Disasters (WIISARD)"
Leslie Lenert, Ph.D, Professor at University of California, San Diego School of Medicine; Associate Director of Bio-medical Informatics for the California Institute for Telecommunications and Information Technology (CALIT2).

**October 6, 2005**
"Crime On The Internet: SPAM, BOTS, and Phishers"
David Aucsmith, Senior Director of Microsoft’s Institute for Advanced Technology in Governments.

**October 25, 2005**
"The Future of Terrorism: Trends and Implications"
Raphael Perl, Senior Terrorism Analyst with the Congressional Research Service, Washington, D.C.

**November 1, 2005**
"International Biosecurity: Finding a Balance"
David R. Franz, D.V.M., Ph.D., Vice President & Chief Biological Scientist, Midwest Research Institute Director; National Agricultural Biosecurity Center, Kansas State University; Deputy Director, Center for Emergency Care & Preparedness, University of Alabama at Birmingham.