

## From Our Director

### The new ISTS

Welcome to this second issue of the ISTS newsletter. As the new Executive Director of ISTS, I am pleased to announce a new structure for ISTS and its research programs. As part of a strategic plan completed this spring, ISTS is now comprised of three centers. Inside this issue you can read about the Cyber Security and Trust Research Center's projects on worm detection, public-key infrastructure, digital tampering, and the Emergency Readiness and Response Research Center's project on sensor and network technologies to support first responders. The Cyber Security Exercise Development Center was responsible for October's Livewire exercise covered in the previous newsletter.

ISTS was founded at Dartmouth in March 2000 and has received major funding from the Office of Domestic Preparedness (Department of Homeland Security) and the National Institute of Justice (Department of Justice), as well as other federal and corporate sources.

ISTS is also a member, and chair, of the Institute for Information Infrastructure Protection (I3P), a consortium of 24 leading academic institutions, non-profits and federal laboratories collectively and collaboratively addressing open issues concerning the safety, security, and robustness of the nation's information infrastructure.

There are currently 17 faculty, 45 researchers and 45 students actively involved in ISTS research activities. Martin Wybourne, the Executive Director of ISTS for 2003-04, is now Dartmouth's Vice Provost for Research.

This issue of the ISTS Quarterly covers a broad range of activity at the institute and news from the I3P. More details can be found on the recently revamped website [www.ists.dartmouth.edu](http://www.ists.dartmouth.edu) and on [www.thei3p.org](http://www.thei3p.org).

Photo: Joe Wehling '69



David Kotz,  
Executive  
Director

## Virtual Academy Prepares Responders for WMD Attacks

By Tim Elliott

Dartmouth's Interactive Media Laboratory (IML), which is supported by ISTS, has entered the home stretch on its interactive terrorism response trainer, called the Virtual Terrorism Response Academy (VTRA).

Hazardous material experts, including John Eversole, retired chief of special operations for the Chicago Fire Department, lead VTRA's first course, "Ops-plus for WMD Hazmat." The course is designed for fire, EMS and law-enforcement personnel trained at the operations level of a national hazardous materials standard.

Joseph V. Henderson, MD, has been director of the Interactive Media Laboratory for 15 years. He's been putting "Ops-plus for WMD Hazmat" through its paces with the nation's top hazardous materials response teams. In May and July, Henderson demonstrated finished simulations related to dirty bombs. The first course's other simulations will address chemical, biological, nuclear and incendiary attacks.

Henderson said VTRA's mission is vital. "We're teaching firefighters, police officers and EMS personnel how to recognize terrorist attacks, respond to incidents properly, and protect themselves and members of their communities," Henderson said. "The distance learning approach offers a means to reach millions of first responders right where they serve."



Sim Room for Simulation #2. Trainee must use Ludlum radiation meter to check anteroom for background radiation levels. Note meter readout in left lower area of the screen. Dosimeter reading is in the right upper corner.

### How does it work?

Trainees enter the VTRA and travel through its halls guided by instructors who are simultaneously master practitioners and master trainers. Chief Alan Brunacini, James O. Page and Gordon J. Graham act as mentors for fire, EMS and law-enforcement audiences, respectively.

The Hazmat Learning Lab provides interactive reviews of various hazmat principles. Topics include the use of instruments and personal protective equipment (PPE), triage and casualty care and crime scene management. A final exercise tests the trainee's grasp of the fundamentals; a passing score rewards the trainee with a key to the Simulation Area.

The Simulation Area is a suite of rooms where trainees get briefings and select PPE and instruments. Then the trainees enter a simulated 3-D space where they must deal with various situations related to WMD-Hazmat (above). The exercise is completed under the guidance of Greg Noll, a master hazmat trainer, who functions as a coach. A debriefing and discussion follows, which helps the trainees learn from their decisions during the simulation. The expected release date is February 2005.

For more details about the program, please go to <http://iml.dartmouth.edu/education/pcpt/index.html>.

## Investigating digital images

By Sue Knapp

What's real and what's phony?

"Seeing is no longer believing. Actually, what you see is largely irrelevant," says Dartmouth Professor Hany Farid, whose research is supported by ISTS. He is referring to the digital images that appear everywhere: in newspapers, on Web sites, in advertising, and in business materials, for example.

Farid and Dartmouth graduate student Alin Popescu have developed a mathematical technique to tell the difference between a "real" image and one that's been fiddled with. Consider a photo of two competing CEOs talking over a document labeled "confidential - merger," or a photo of Saddam Hussein shaking hands with Osama bin Laden. The Dartmouth algorithm, presented recently at the 6th International Workshop on Information Hiding, in Toronto, Canada, can determine if someone has manipulated the photos, like blending two photos into one, or adding or taking away objects or people in an image.

continued on page 2

“Commercially available software makes it easy to alter digital photos,” says Farid, an Associate Professor of Computer Science. “Sometimes this seemingly harmless talent is used to influence public opinion and trust, especially when altered photos are used in news reports.”

A digital image is a collection of pixels or dots, and each pixel contains numbers that correspond to a color or brightness value. When marrying two images to make one convincing composite, you have to alter pixels. They have to be stretched, shaded, twisted, and otherwise changed. The end result is, more often than not, a realistic, believable image.

“With today’s technology, it’s not easy to look at an image these days and decide if it’s real or not,” says Farid. “We look, however, at the underlying code of the image for clues of tampering.”

Farid’s algorithm looks for the evidence inevitably left behind after image tinkering. Statistical clues lurk in all digital images, and the ones that have been tampered with contain altered statistics.

“Natural digital photographs aren’t random,” he says. “In the same way that placing a monkey in front of a typewriter is unlikely to produce a play by Shakespeare, a random set of pixels thrown on a page is unlikely to yield a natural image. It means that there are underlying statistics and regularities in naturally occurring images.”

Farid and his students have built a statistical model that captures the mathematical regularities inherent in natural images. Because these statistics fundamentally change when images are altered, the model can be used to detect digital tampering.



Photo: Joe Mehling '69

Hany Farid

## I3P News

### Security in the News Moving to the I3P Knowledge Base

**S**ecurity in the News, launched in October 2001, is a daily cyber security and critical infrastructure protection news summarization service.

The number of subscribers has steadily grown to approximately 3,000, and the service is mirrored by dozens of government and industry organizations around the world.

Security in the News began as an internal ISTS e-mail service, but soon became a thriving public service. It is a one-stop-shop for comprehensive, timely and accurate security news. According to the editor, Eric Goetz, the real value to users – and what distinguishes it from other similar offerings – are the story summaries that give readers a brief overview of the day’s events, while letting them decide which articles they want to peruse in more detail.

Current subscribers are people in the US military, within the homeland security community, at academic institutions, with technology and Fortune 500 companies, or

from the media. Subscribers also hail from scores of countries. The Security in the News web page gets over 1,000 visitors per day on average, and the site is used by dozens of organizations in government and the private sector, including the New York State Office of Cyber Security & Critical Infrastructure Coordination, Japan’s National Police Agency and the SANS network’s Internet Storm Center.

With the switch to the I3P, Security in the News will be an integral part of the I3P Knowledge Base. The KB will present a portfolio of cyber security information offerings, which will also include weekly Law & Policy and Research & Development news updates, an events calendar, funding opportunities information, collaboration space for researchers and, eventually, a digital archive.

To subscribe, visit Security in the News at the I3P website at [www.thei3p.org](http://www.thei3p.org).

## DIB:S System Allows Early Warning of Worm Attacks

**I**STS researcher Bob Gray is hunting worms. He and his colleague Vincent Berk have developed a way to monitor routers, the hubs and intersections of the Internet, to detect evidence of a worm attack.

The majority of worm attacks on vulnerable systems are carried out by malicious processes randomly generating large numbers of IP addresses, blindly probing these selected addresses, and finally attempting to exploit vulnerabilities on those hosts that respond to the probes. Data gathered up to and including the Code Red and Nimda worms indicate that the vast majority of these probes never reach their addressed destination. Indeed, over 80% of all responses to blind attack probes are router-generated ICMP Host or Network Unreachable messages. ICMP, the Internet Control Message Protocol, is a set of standards by which devices speaking IP (Internet Protocol) can tell each other about

the status of communications. Routers, subject to a per-second rate limit, will generate ICMP Unreachable messages if they do not know how to route a packet to its destination (for example, if the host is unreachable or an entire address block is unused).

Most current worms, such as Code Red v2 and Sapphire/Slammer, find vulnerable machines through exactly this kind of probing or scanning process. As the worm propagates, it attempts to contact many unreachable addresses, causing Internet routers to generate many ICMP Unreachable messages. In addition, the number of generated ICMP messages increases in proportion to the number of infected hosts, making the messages a useful data source for worm detection.

The DIB:S prototype (Dartmouth ICMP Bcc: System) collects ICMP messages from instrumented routers, and uses three different techniques to determine whether the

message pattern indicates a propagating worm. A small number of instrumented routers can provide good detection of worm activity.

Current work focuses on real-world deployment, as well as a more detailed analysis of detection performance. Real-world deployment will hopefully be aided by a partnership with Cisco, which has incorporated the necessary ICMP-forwarding functionality into a beta version of their Internetworking Operating System (IOS) software. Cisco IOS Software controls many Internet routers and other network devices.

Readers interested in participating in the worm-detection system by deploying their own instrumented router (or providing other scan data) can contact ISTS researcher Bob Gray at [robert.s.gray@dartmouth.edu](mailto:robert.s.gray@dartmouth.edu).

More details about DIB:S can be found on the ISTS website under Cyber Security & Trust Research Center (CSTR) ‘Project Description.’

# Building Bridges in Higher Education

By Scott Rea & Steve Worona

Three of the most important concerns for users of large business networks, such as those at institutions of higher education or medical facilities, are security, privacy and identity. How do we keep viruses, worms and spam from crippling our computers and networks? How do we ensure that patients' medical records and consumers' financial information don't fall into the wrong hands? How do we know that the person connecting to our campus network is an authorized member of the community? How do we know that the data associated with a given transaction was not modified en route as it traversed unprotected networks?

According to Mark Franklin, Project Manager in Dartmouth's PKI Lab, one of the most promising approaches to ad-

ressing these concerns is Public Key Infrastructure (PKI), which provides, in a single technology, a mechanism to prove identity, and to sign or encrypt documents and data.

Higher education institutions, business and government are implementing PKI for their internal use, and a service called a Bridge Certificate Authority (BCA) establishes trust and addresses security, privacy and identity concerns between subscribers to different PKIs across institutional boundaries. A BCA provides a translation point between different PKIs allowing the subscribers of one PKI to trust the credentials (at a specified level of assurance) issued by a different PKI.

Researchers in Dartmouth's PKI Lab, an affiliated project of ISTS's Cyber Secu-

rity and Trust Research Center, are now designing and building a Higher Education BCA (HEBCA). EDUCAUSE, representing the information technology leadership of higher education, received support from the American Council on Education and the National Association of College and University Attorneys, to implement a Higher Education BCA (HEBCA), and they turned to Dartmouth for help.

The Dartmouth team will not only create HEBCA, but it will also deploy it and operate it from Dartmouth's computing facilities. In time, the HEBCA will link with other PKI bridges operated by government and commercial organizations, further extending the reach of PKI technology and the trust infrastructure for higher education institutions.

## ISTS Researchers Build Ties with First Responders

One of the goals of the newly formed Emergency Readiness and Response Research Center

(ER3C) is to pursue technologies that can be used by first responders to improve situational awareness. ER3C researchers on the First Responder (FR) Sensor project are developing technologies focus on environmental and physiological sensing and information management. Through the remote sensors, responders, casualties and the environment can be monitored to form a view of the scene that will improve the response effort and hopefully save lives. The FR Sensors research team, led by Sue McGrath, Director of the ER3C, had the opportunity to gather domain knowledge and field experience by spending some time recently with first responders in local, regional and national communities.

In March of 2004, members of the ER3C team participated in Tactical Emergency Medical Service (EMS) training in Chelmsford, Mass. During this event they observed medical personnel train to perform their duty in high-risk situations, including working with a SWAT (Special Weapons and Tactics) team on a simulated house entry mission. This event provided the team with knowledge about procedures for remote triage and will influence the design of

the health state classification algorithm in their physiological monitoring system.

A few months later in June 2004, two

team members, Michael De Rosa and Aaron Fiske, participated in a simulated rescue mission at the Bourne Bridge in Cape Cod, Mass. During the exercise, De Rosa and Fiske recorded physiological sensor data from two volunteers, confirming the system's ability to wirelessly stream physiological

data from users under emergency conditions, establish multi-hop ad-hoc links over several hundred feet, and qualitatively evaluate the effect of structural steel members on 802.11 and GPS wireless reception.

The ISTS team continues to develop emergency response scenarios that will explore the performance and limitations of the FR Sensor project technologies. Chris Carella, Research Associate, has created one scenario that involves a chemical spill after a train derailment. To learn about the likely response to such an event, Carella and Lori Terino, Research Associate, met with various state and local first responders in June 2004, including the Louisiana State Police, East Baton Rouge Parish Office of Homeland Security and Emergency, the Baton

Rouge Fire Department, Ascension Parish Office of Homeland Security, and the Exxon emergency response department. Louisiana is an especially important region for this type of exercise, because sixty percent of the United States' hazardous materials are created, refined or transported through Baton Rouge. The relationship with the Baton Rouge responders was facilitated by ISTS membership in the InterAgency Board (IAB), a national first responder organization.

The FR Sensor project team's experience with local, state and national emergency response personnel has proven to be extremely valuable in helping refine research on systems that will provide first responders with new and improved tools and technology for their jobs.



Photo: Joe Wehling '06

Left to right: Mike DeRosa '03, Suzanne Wendelken Th '04, Director of ER3C Sue McGrath and Aaron Fiske '02



Photo: Michael De Rosa '03

Aaron Fiske rappels down the concrete pier at the Bourne Bridge EMS training in July. Fiske and Mike De Rosa used two of the FR Sensor physiological monitoring systems to gather data from responders during the event. The tests provided valuable information about the configuration and operation of the current testbed system.

Institute for Security Technology Studies at Dartmouth  
(A national center for cyber and homeland security research and development)  
45 Lyme Road

Hanover, NH 03755-1219

phone: (603) 646-0700

fax: (603) 646-0660

email: [info@ists.dartmouth.edu](mailto:info@ists.dartmouth.edu)

[www.ists.dartmouth.edu](http://www.ists.dartmouth.edu)

## ISTS and i-SAFE America By Sondra Walker

As we all know, a secure Internet is a boon to business, and a valuable communications and learning tool for people of all ages. Unfortunately, some people also use it to invade the privacy of others, defraud the unsuspecting, or trick vulnerable users into giving vital personal information through e-mail or online chat rooms.

Congress recognized these dangers and has funded a national, non-profit, Internet safety education foundation, i-SAFE America, to provide curricular materials and awareness programs to every state. According to i-SAFE, recent surveys show that young people who use the Internet regularly have received an aggressive solicitation to meet a cyber "friend" in person. Another study referenced by i-SAFE reveals that more than 50 percent of youth do not recognize the potential risks related to meeting in person with someone they met online.

ISTS recently joined with i-SAFE America to hold a Town Meeting at Dartmouth to provide parents, students, teachers, school administrators and resource officers, and others throughout the community with the opportunity to hear more about these issues, and to learn how to provide students and other vulnerable parties with the information and decision-making skills they need to recognize and avoid dangerous and/or unlawful online behavior.

The July 16 Town Meeting opened with a panel discussion by ISTS and i-SAFE representatives, including a retired FBI agent who now chairs the i-SAFE America Board, and a Keene, NH, detective who is known internationally for his work in tracking down criminals in this field. A question and answer session closed the meeting as community members engaged in discussions about the technical, social, and educational solutions for improving Internet safety and security. For additional information see <http://www.isafe.org>.



## Grants & Awards



Sean Smith and his Public-Key Infrastructure (PKI) team received two grants: One \$40,000 grant from Sun Labs will augment both the research and the deployment missions of the PKI Lab. The second, a \$72,000 grant from Intel's University Research Council, is to extend the Greenpass project.

## News from an Alum

Many of us remember Geoff Stowe, who interned at ISTS from June 2003 until his graduation from Dartmouth in June 2004. During that time he was responsible for designing and implementing the security system required for Livewire, the first national cyber security exercise. Using security knowledge taught at Dartmouth he put theory to practice to guard and protect access to the exercise. Geoff's hard work and study under academic leaders in Cyber Security and Computer Science during his four years at Dartmouth led him to his current job where he is working in the Computer Forensics and Intrusion Analysis group at a Northern Virginia defense contractor doing technical research in national security fields. Congratulations to Geoff.