The Institute for Security Technology Studies (ISTS): overview

David Kotz*

The Institute for Security Technology Studies
Dartmouth College, Hanover, NH, USA 03755

ABSTRACT

The Institute for Security Technology Studies (ISTS) was founded at Dartmouth College in 2000 as a national center of security research and development. The Institute conducts interdisciplinary research and development projects addressing the challenges of cyber and homeland security, to protect the integrity of the Internet, computer networks, and other interdependent information infrastructures. ISTS also develops technology for providing the information and tools necessary to assist communities and first responders with the evolving, complex security landscape. ISTS is a member of and administers the Institute for Information Infrastructure Protection (I3P), a consortium of 24 leading academic institutions, non-profits and federal laboratories that brings industry, academia and government together to articulate and focus on problems that need to be solved to help ensure the nation's information infrastructure is safe, secure, and robust.

Keywords: Dartmouth College, cybersecurity, emergency response and preparedness, information infrastructure protection

1. INTRODUCTION

The interdisciplinary ISTS teams of academic scholars and professional scientists seek to investigate critical security problems both through the creative application of existing technology and ideas, as well as through the discovery of new knowledge and the development of new technology. The interdisciplinary nature of the teams allows ISTS to tackle problems from a variety of perspectives including science, engineering, social science, and policy.

The focus of ISTS research is advanced technology to protect the integrity of the Internet, computer networks, and other interdependent information infrastructures. ISTS also addresses topics related to bio-terrorism and is developing sophisticated tools for first responders, including communications, physiological monitoring, simulation, and training. ISTS involves over 100 faculty, students and staff, including researchers from Dartmouth's College of Arts & Sciences, Thayer School of Engineering, Dartmouth Medical School, and the Tuck School of Business. ISTS has 12 ongoing research programs and 26 major projects completed. Since inception, over 90 researchers and 55 undergraduate and graduate students have contributed to ISTS initiatives.

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. The consortium brings industry, academia, and government together to address open issues concerning the safety, security, and robustness of the nation's information infrastructure.

The ISTS was founded in 2000 under cooperative agreement with the National Institute of Justice at the Department of Justice. Following the creation of the Department of Homeland Security (DHS), program management of ISTS was transferred to the DHS Office for Domestic Preparedness in July 2003.

This paper provides an overview of recent ISTS projects. For further information, see the ISTS web site at www.ists.dartmouth.edu.

* Director of Research and Development. Email: dfk at cs.dartmouth.edu. http://www.ists.dartmouth.edu/

2. RECENT HIGHLIGHTS

2.1. Livewire National Cyber Exercise

ISTS designed and directed the Livewire National Cyber Exercise, at the request of the Homeland Security Council, in October 2003. ISTS enlisted stakeholders in the local government, private, federal, and international sectors to participate in this exercise, designed to explore the challenges of responding to a large-scale, sustained cyber attack directed against the nation's telecommunications, energy, banking, and finance sectors. Within the computer-based simulation built for the exercise, ISTS launched a series of scripted network attacks against simulated player networks. The exercise engaged about 300 people from 50 organizations in government and industry in 14 locations across the nation. The exercise was completed successfully, and an After Action Report was recently delivered to the players. Furthermore, data collected during the exercise provides the foundation of research by Assistant Professor of Sociology Denise Anthony, who is interested in inter-organizational communication patterns. ISTS is preparing for briefings at the national level on the implications of the first Livewire Exercise.

2.2. TOPOFF II (cyber-attack exercise)

The TOPOFF II exercise was a congressionally-mandated exercise conducted in Seattle and Chicago in May 2003. ISTS was asked to conduct a simultaneous cyber exercise, and enlisted a number of other stakeholders in the local government, private, federal, and international sectors to participate. Within the computer-based simulation built for the exercise, ISTS launched a series of scripted network attacks against simulated player networks. The cyber exercise was completed successfully, and an After Action Report was delivered to the Office for Domestic Preparedness at the end of July 2003.

2.3. Cyber crime workshop

ISTS brought national cyber attack experts to New Hampshire in July 2003 to help prioritize the research and development needs for investigating and prosecuting cyber attackers. The results of ISTS research in this domain will be published in a *Law Enforcement Tools and Technologies for Investigating Cyber Attacks: a National Research and Development Agenda* in early 2004. Practitioners and expert reports alike have called for a published research and development agenda to help researchers understand the problems law enforcement faces that may be addressed by research and development. The Technical Analysis Group of ISTS brought law enforcement, private sector, and academic practitioners together for the purpose of prioritizing the research and development areas previously identified in the 2002 publication *Law Enforcement Tools and Technologies for Investigating Cyber Attacks: A National Needs Assessment* such as circumventing encryption, automated log analysis, and detecting IP spoofing. Participants included individuals from the Department of Justice, the Federal Bureau of Investigation, the United States Secret Service, NASA, the New Hampshire Attorney General's Office, the National Law Enforcement and Corrections Technology Center, the National White Collar Crime Center, and investigators from New York, Florida, California, and South Carolina, as well as the San Diego Supercomputer Center at the University of California, San Diego, and the University of New Haven.

2.4. *Survey and Analysis of Security Issues in the U.S. Banking and Finance Sector*

This report released by ISTS in September 2003 examines the security of the banking and finance industry, one of thirteen critical infrastructure sectors identified by the Department of Homeland Security. The report asserts that the banking and finance sector is perhaps the most advanced of all the sectors in adopting defensive measures against terrorism and other threats; however, it remains vulnerable to certain types of attack. This report, intended primarily for policy makers, highlights past and ongoing security efforts at individual companies and sector wide, and provides a clear, concise, and timely overview of the current state of the security of the financial services industry. Available on the ISTS web site, this is the fourth in a series of Institute papers studying the security of critical infrastructures. Past reports examined information and telecommunications systems, the electric power industry, and transportation systems.

3. ACADEMIC PROGRAMS & OUTREACH

3.1. Research fellowships

The Institute initiated a residential research fellowship program in the fall of 2002 to expand the depth and breadth of its research portfolio. In its call for proposals, ISTS sought to draw interest from researchers and scholars in academic, government, and industry settings. Candidate selection was tied to (1) the applicants' record of academic achievement (2) the quality and promise of the proposed research and (3) the prospect for the proposed work to advance the mission of the Institute and make significant contributions to security technology studies. Successful candidates were identified based on the way in which their work would support and extend interdisciplinary research being advanced at ISTS.

The search led to the appointment of the following fellows:

- Senior Researcher Scott Borg's research focuses on determining the business costs of cyber attacks.
- Postdoctoral Fellow Zack Butler investigates algorithms for positioning and organizing mobile sensors in response to events in their environment.
- Senior Fellow Scott Dynes focuses on the business case for cybersecurity and explores the economic drivers of cybersecurity within organizations.
- Postdoctoral Fellow Michael Freeman examines connections between terrorism and technology, explores policy options for reducing vulnerabilities, analyzes how democracy and terrorism affect each other, and studies how fighting terrorism affects civil liberties in democracies.
- Postdoctoral Fellow Tristan Henderson manages an effort to collect and analyze extensive data about the traffic on the Dartmouth campus wireless network, including an estimate of the impact of worms and other attacks.

In addition to advancing their own research, ISTS fellows are expected to interact with other national and local researchers, Dartmouth faculty and students; participate in seminars and other events sponsored by the Institute; present technical talks, and produce a paper of publishable quality, based on the research conducted during their residency.

3.2. Outreach

The Institute sponsors two regular speaker series. A series of internal speakers reports on work in progress at the Institute, aimed at raising awareness of current research activities within ISTS and the Dartmouth community. A series of external, invited speakers brings in outside perspectives and provides an opportunity for Dartmouth faculty, students, and staff to learn about the broader aspects of cyber and homeland security.

4. RESEARCH

The primary mission of ISTS is to conduct a range of basic and applied research into the technology challenges surrounding cyber and homeland security. Although its primary focus is cybersecurity, ISTS also studies technologies designed to support emergency response. In this section, some recent projects are briefly summarized; for more information please see the ISTS web site.

4.1. Kerf toolkit for intrusion analysis

The objective of this project is to provide computer system administrators with new methods for the analysis of attacks on their computer system. Numerous intrusion-*detection* tools exist; Kerf's focus is on intrusion *analysis*, specifically, tools that help administrators to examine large amounts of host and network log data. The Kerf tools will fit into the unexplored territory between current approaches that search log data without providing much context and those that report summary statistics about records within the logs.

Given that an intrusion has been detected, the Kerf tools help the administrator answer basic questions about the attack: How, when, and where did the intruder get in? What did the intruder do here? Where did the intruder come from? Did the intruder attack remote machines using my system? Answering these questions allow the administrator to close security holes, determine damage, and collect evidence that may lead to the discovery and capture of the intruder.

4.2. MEMS for infosecurity

Using microscopic devices built with MEMS (Microelectromechanical Systems) technology as a new approach towards data security, ISTS investigates application of MEMS technology to create a digital medium whose contents can be verified by non-electronic means. The research intends to create an instrument that protects computer systems from attacks launched by simple insertion of digital medium (floppy, CD, DVD) into a reader and uses MEMS technology to create a medium whose contents can be checked for a digital signature, through MEMS rather than electronically.

4.3. Process query systems for homeland security

The main technical objective of this project is to develop advanced capabilities of Process Query Systems (PQS) for specific use in Homeland Security data analysis (HSDA) problems. PQS is a novel software system (that is being developed at Dartmouth) capable of accepting *process* descriptions as queries. A PQS then performs standing queries and searches against databases and datastreams of sensor reports for evidence that instances of the queried processes exist in the data. The basic concepts underlying a PQS are derived from the mature theory and substantial implementation experience of multiple-hypothesis, multiple-target tracking in radar and sonar signal processing.

ISTS researchers believe that an appropriately designed and implemented Process Query System has the potential to revolutionize HSDA in ways that incremental research and development cannot and will not. This project will gain experience with an alpha version of a PQS for select HSDA problems, to evaluate the resulting performance, and to develop a distribution-quality PQS for government use.

4.4. Synthetic environment simulation for emergency response

A terrorist attack, disaster, or other large-scale emergency requires a coordinated response from multiple first responder organizations at the local, state and federal levels. Mission rehearsal is critical to a successful response. A coordinated response also depends on the existence of robust and efficient command-and-control (C2) software systems, such as communications middleware and visualization, planning, and decision-making tools. Of course, testing such software to ensure its robust and efficient operation, and adequately training first responders and commanders in its use, should be done *before* a disaster actually occurs. Live exercises can be used for training and evaluation of equipment, but the expense and time associated with deploying real people and real equipment for live exercises are often prohibitive. Ideally, emergency plans, procedures, and software systems could be tested using a proxy for reality; a synthetic environment.

To address this problem, this project will leverage the synthetic environment approach employed in many military training applications, and will develop an extensible framework that can use a virtual emergency to exercise a real civilian C2 software system (or to train human first responders in the use of that system). A synthetic environment is a collection of computer simulations that together form a digital approximation of the anticipated environment for the real system. The component simulations include terrain, buildings, atmospheric effects, human behavior, and communication channels.

4.5. Emergency first responders—an integrated approach to communication, automated information management, and sensing for emergency and disaster response

Imagine a disaster and emergency response system that can improve our nation's ability to react to such events. This project contributes to solving three critical challenges: reliable communications, environmental and physiological sensing, and automated information processing. This research will explore new methods to integrate sensor networks, information-fusion middleware, ad hoc wireless networks, and physiological monitoring algorithms. The goal is to provide the foundation for a system that provides better situational awareness to first responders, to incident commanders at the scene and at remote coordination centers, and to hospital emergency workers.

The key to this research plan is an integrated development approach that includes algorithm development, simulation, hardware implementation, and field testing. This project complements other systems currently under development, such as the Disaster Management Interoperability Services effort sponsored by the Federal Emergency Management Administration. Project leaders are involved in organizations such as the InterAgency Board for Equipment Standardization and Interoperability, which will help them to transfer the ISTS technology into emergency response systems at the local, state, and federal levels.

4.6. Analysis of data-collection capabilities of a large-scale, distributed honeypot system

A Distributed Honeypot System can be defined as a collection of honeynets or honeypots that are distributed throughout the Internet or other large network and that send their data to a central analysis point. Such a system can play a critical intelligence-gathering role for network defenders, since it will observe a broader range of attack activity than a single honeypot or honeynet, and can capture more information about each attack than traditional intrusion-detection systems. The Distributed Honeypot System could provide reliable detection of attacks directed against the Internet or other network, early warning of new attacker tools, methodologies and techniques across a wide range of attacker types, and *extensive* attack data that can be analyzed as a first step toward developing preventive and defensive measures. Current honeypot technologies require significant manual oversight, however, limiting abilities to make a large-scale deployment. Moreover, it is not yet clear how broad an attack picture a large-scale honeypot deployment will actually see. Will every honeypot in the system see similar attacks from attackers with similar skill levels?

This project is examining the automation of honeypot functionalities to reduce, albeit not eliminate, the need for manual oversight, and will analyze the usefulness of a distributed honeypot system as a large-scale intelligence-gathering tool. Specifically, ISTS researchers will deploy and operate a distributed honeypot involving multiple types of honeypots at multiple types of organizations, collect attack data from these deployed honeypots, and systematically analyze that data to determine the breadth and depth of attack activity directed against the distributed honeypot system.

4.7. Dartmouth ICMP bcc: system (DIB:S)

Most current (non-email) worms propagate by 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. As such a worm propagates; it attempts to contact many unreachable addresses, causing Internet routers to generate ICMP Unreachable messages. The DIB:S (Dartmouth ICMP Bcc: System) prototype collects ICMP messages from instrumented routers, and uses three different techniques to determine whether the message pattern indicates a propagating worm. In addition, DIB:S detects general scanning activity, and models could be developed to identify the traffic patterns associated with other distributed attacks besides worms. Current work focuses on the effect of different kinds of noise on the detection techniques and on real-world deployment of the DIB:S system. Deployment is 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.

4.8. Information security

This project takes place within the broader scope of the Dartmouth Public-Key Infrastructure (PKI) Lab. The Lab's goal is to examine why PKI has not yet achieved its potential to enable robust expression of non-trivial, compound statements and beliefs, among entities that share no common secrets (something important to the emerging distributed information world). The lab receives support from several sources: besides ISTS, it is also funded by the Mellon Foundation, Internet2, Cisco Systems, and the National Science Foundation, as well as an equipment loan from IBM Research. Within the lab, there are two teams: the Deployment Team is examining how to integrate PKI within electronic processes at Dartmouth; the Research Team is looking at the missing pieces. The end goal is to move the research products into deployment in a series of increasingly large pilots. In the near term, researchers are exploring keyjacking analysis and potential solutions, an analysis of architectural support for secure computing, and the use of PKI techniques to support guest authorization in wireless networks.

4.9. Detecting digital tampering

The ease with which digital media can and is being manipulated and altered is stunning. At least one consequence of this 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 speed, 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.

To this end, an ISTS team has developed several statistical tools to detect various forms of digital tampering (in the absence of digital watermarks or signatures). Their approaches work on the assumption that although tampering may leave no visual clues, it may, nevertheless, alter the underlying statistics of an image. They have also developed a

general statistical model that can differentiate between photographic and computer generated images, detect hidden messages embedded within digital images, and protect biometric systems against re-broadcast attacks.

4.10. Efficient production of catalysts to detoxify nerve agents

The threat of biological and chemical weapons of mass destruction mandates the development of highly effective methods to neutralize such agents in the event of an attack. One class of biological and chemical weapons of mass destruction in particular, the organo-phospho compounds (e.g., Sarin, Tabun, and Soman), are of concern since their availability and ease of deployment has already been demonstrated. Several biological catalysts are known that can effectively hydrolyze and thereby destroy organo-phospho compounds. One such enzyme, the organo-phospho hydrolase from *Pseudomonas diminuta,* is the focus of ISTS work. The ultimate goals are to improve cleanup (for example, to detoxify exposed equipment) and protection (for example, to improve air filters used in buildings or personal protective equipment).

The goal of the research is to develop a stable Organophosphohydrolase (OPH) expression system and to develop a cheap and efficient protein recovery system. In 2000, ISTS researcher Tillman Gerngross co-founded GlycoFi, Inc., a company pioneering the "humanization" of yeast and fungal protein expression systems and the commercialization path for the protein recovery system. Simultaneously, several projects are underway to improve recombinant protein recovery by engineering at the molecular level.

4.11. Removal of toxins and pathogens using human monoclonal and bispecific antibodies

Anthrax, particularly inhalation anthrax, is a deadly disease that has already been used in a biological attack against Americans. An ISTS team is working to develop new antibodies that, if eventually approved for clinical use, could be used to protect a first responder or health care worker at or even soon after the time of exposure. It may even have therapeutic benefits for patients already infected. A pre-clinical study funded in part by ISTS was conducted with the U.S. Army Medical Research Institute of Infectious Diseases and Medarex, Inc. to determine both the minimal amount of a fully human antibody required to protect against anthrax as well as the antibody's therapeutic activity when given at the time of anthrax inhalation. The antibody, MDX-1303, provided rabbits with full protection against inhalation anthrax at the lowest dose tested, 1 mg/kg and reduced mortality even when administered 1-2 days after inhalation, once animals displayed signs suggestive of disease.

MDX-1303 is a fully human antibody against the inhalation anthrax, the most lethal form of illness in humans caused by the *Bacillus anthracis* bacterium, and targets a protein component of these lethal toxins known as the anthrax protective antigen. The anthrax protective antigen initiates the onset of the illness by attaching to cells in the infected person, and then facilitates the entry of additional destructive toxins into the cells. MDX-1303 is designed to target the anthrax protective antigen and protect the cells from damage by the anthrax toxins. The results indicated that all doses tested were protective in rabbits exposed to lethal doses of anthrax spores by inhalation. The results also demonstrated that administration of MDX-1303 to rabbits 24 or 48 hours after exposure to anthrax could result in recovery and survival of the animals without the addition of antibiotics. These results suggest that the MDX-1303 antibody has the potential to be developed both as a prophylactic to protect people at risk of exposure to anthrax, such as first responders or unvaccinated military personnel, and as a therapeutic for patients already showing signs and symptoms of anthrax infection. The finding that the antibody is therapeutic suggests that it has the potential to augment antibiotic treatment, which by itself is poorly effective in symptomatic infection.

4.12. Virtual terrorism response academy

The Program on Counterterrorism Preparedness and Training (PCPT) works to develop training products and supporting infrastructure to promote counterterrorism preparedness among first responders at local, state, and federal levels. PCPT's principal research is in the production of the Virtual Terrorism Response Academy, a low-cost, high-impact training for WMD response. The Quake II-based simulations feature real-world instruments and physics in a 3D game engine on high-quality streaming video to create a sense of immersion in a real-world scenario.

In collaboration with John Eversole, widely regarded as the premiere authority on hazardous-materials training in the country, and other members of an advisory council, the program's direction has been enhanced to help educate for "Ops Plus" training. This is a completely new area of response to WMD and, as a result, PCPT is acting as a pioneer with other partner members of the Center for Domestic Preparedness to help create this new paradigm. This new area of

"Ops Plus" training will enhance any first responder who is trained to an "Operations" level, and give the first responder community another tool in the terrorism response toolbox.

4.13. Technical analysis group

The mission of the Technical Analysis Group (TAG) is to identify, report, and address specific national law enforcement priorities. This effort is critical given the role of law enforcement in preventing and responding to physical terrorism or cyber attacks. With guidance from national experts, TAG has examined, prioritized, and published operational requirements and informative non-classified intelligence products.

4.13.1. Law enforcement tools and technologies for investigating cyber attacks

Responding to the need for law enforcement specific research, expressed by a number of authoritative reports, TAG developed a three-phase approach to identifying, validating, and reporting the technological impediments facing law enforcement when investigating and responding to cyber attacks, for which research and development might provide solutions. As a first step, TAG published *Law Enforcement Tools and Technologies for Investigating Cyber Attacks: a National Needs Assessment* in June 2002. The *National Needs Assessment* provides a comprehensive look at the problems and technological impediments facing federal, state, and local law enforcement when investigating and responding to cyber attacks. The second step was to identify available technology solutions that purported to address the requirements revealed in the *National Needs Assessment*. ISTS mapped the collected tools against the needs, based solely on manufacturers' claims, to determine where "gaps" in product availability may exist and published *Law Enforcement Tools and Technologies for Investigating Cyber Attacks: Gap Analysis Report* in March 2004. The third and final stage is publication of the prioritized needs based on the prioritized, unsatisfied needs revealed during a working group convened in July 2003. ISTS plans to publish this *Law Enforcement Tools and Technologies for Investigating Cyber Attacks: a National Research and Development Agenda* in 2004.

4.13.2. Prototype national contact index for cyber attack investigators

A *Prototype National Contact Index for Cyber Attack Investigators* is undergoing testing and evaluation. This national index lists contact information for people involved in the investigation and prosecution of cyber crimes. The index, which is restricted to law enforcement, facilitates outreach and communications with colleagues nationally.

4.13.3. "Open-source" products

There is clear, factual evidence that Islamic terrorist groups are using information technologies to facilitate propaganda, recruitment and training, fundraising, communications, and targeting operations. Discussions between law enforcement, the private sector, and academia revealed that there is a lack of authoritative, publicly available unclassified materials concerning the use of cyber technology by Islamic terrorist groups. (Such publicly-available information gained from news, academic, and other sources is referred to in the intelligence community as "open-source.") To meet this need, the Technical Analysis Group at ISTS has detailed how cyber technologies are exploited by these hostile groups in a report titled, *Examining the Cyber Capabilities of Islamic Terrorist Groups*.

5. PRODUCTS

In addition to the above research, most of which led to papers published in the academic literature, ISTS teams have produced many tools, reports, and online course materials. A few are highlighted here.

5.1. Software tools (as of December 31, 2003)

5.1.1. Digital evidence retrieval

This software helps to glean information from images stored on seized computers, such as the make and model of camera used. This cost-free tool for digital evidence retrieval was distributed to all Internet Crimes Against Children task forces and to law enforcement personnel nationwide. It is now used in more than 25 states.

5.1.2. Jeanne: modified reverse proxy server

This project provides a new way of securing web sites through the use of Reverse Proxy Servers. By placing your web server behind a firewall and using this proxy to receive all HTTP requests, it is possible to achieve higher security for your web site.

5.1.3. Universal steganalysis (detection of hidden information)

A computer program licensed to United Devices, Inc. is capable of detecting the presence of hidden messages embedded within digital images. The novelty of the work is in the specific statistical models employed, and in its ability to detect hidden messages independent of the specific image format or hiding technique. This tool provides new technological assistance for cyber investigators in detecting secret communications hidden in digital images between subjects under investigation.

5.1.4. Q-RAN (cybersecurity risk management)

Quantitative Risk Analysis of Computer Networks (Q-RAN), developed by Dartmouth researchers, is both a methodology and a toolset designed to address the problem of risk opacity in networks. Q-RAN allows risk managers to get a detailed and comprehensive snapshot of the technical weaknesses of a network and its constitutive software, assess its risk profile, and propose measures to improve the profile *before* an attack takes place.

5.1.5. Authentication of biometric data

ISTS has developed a technique for distinguishing between an originally recorded image (or audio) and a re-broadcast image (e.g., scanned and re-printed). This technique can protect biometric systems (e.g., face, iris, voice) vulnerable to attacks in which an attacker re-broadcasts a previously made image/recording to the authentication device.

5.1.6. Information security

- Open-source Linux support for hardening web servers with TCPA/TCG available at http://enforcer.sourceforge.net.
- Patches to Mozilla to add a trusted path that prevents malicious server content from spoofing security-relevant metadata from the browser (as well as demos of how to do this spoofing).
- A prototype of SPADE, which uses SDSI-SPKI to construct and maintain attribute release policies in Shibboleth.
- Prototype code for Armored Data Vault, enabling forensic analysis of archived LAN data, but only in a manner which ensures that analysis follows pre-agreed policy.
- Prototype code for a privacy-enhanced credential directory.
- X.C. worm detection and removal tool.
- Adore worm detection and removal tool.
- Lion worm detection tool.
- Ramen worm detection and removal tool.

5.2. Online tutorials

ISTS offers several online tutorials on its web site, ranging from Linux security to early detection of Internet worms. For example, in one course about SSH subtitled, “the Swiss army knife of encryption tools,” basic SSH operation, port forwarding, X Windows forwarding, and the installation and use of SSH keys are covered. Attendees finish with the background needed to start using SSH and SSH keys to encrypt terminal sessions, X applications, and other types of TCP traffic.

5.3. News & information retrieval

Security in the news provides daily dissemination of pertinent open-source cybersecurity intelligence issues and developments in the cybersecurity sector. An email subscription is free at the ISTS web site.

The **CyberSleuth** is an automated, up-to-date intelligence report on recent computer security threats and defenses, eliminating the need for costly and time-consuming manual monitoring or subscribing to pay-for-service sites. CyberSleuth is available for free at the ISTS web site.

6. SUMMARY

Although a young organization, ISTS is a vibrant and active community of researchers involving numerous faculty and students from all schools within Dartmouth College. The focus of ISTS research has been cybersecurity, although the Institute has several projects in Emergency Response and Preparedness (developing better network communications for digital responder assistants, and developing interactive multimedia), and two projects related to developing defensive mechanism to protect first responders when they are faced with a nerve agent or anthrax. More information about all projects is available on the ISTS web site, www.ists.dartmouth.edu.

ACKNOWLEDGEMENTS

This project was supported under Award Number 2000-DT-CX-K001 from the Office for Domestic Preparedness, U.S. Department of Homeland Security. Points of view in this document are those of the author(s) and do not necessarily represent the official position of the U.S. Department of Homeland Security.