

From Our Director

The ISTS mission is to conduct research that addresses critical national needs for security technology and policy in cyber and emergency response environments. The ISTS approach is to address problems of (long-term or short-term) importance to the nation, focus on security technology in cyber and emergency response environments, leverage the strengths of Dartmouth College, produce excellent research and publish in quality academic venues, and impact the "real world" in some way, beyond papers and students. Most of this research is conducted within two centers, one focused on Cyber Security and Trust Research (CSTR) and the other on Emergency Readiness and Response Research (ER3).

In this issue we highlight a wide variety of ISTS projects. We describe recent work in ER3C involving clinical trials that help us to develop new algorithms for interpreting physiological sensor data. Other articles cover cyber security, including a recent report on the cyber warfare capabilities of other nations, a project that develops "honeypots" to uncover the techniques used by attackers that break into computer systems, and system support for trusted hardware platforms.

Finally, the I3P has launched its "Knowledge Base" as a resource to the cyber security and information infrastructure protection research community.

We are particularly excited to announce a new NSF CAREER award for Sean Smith, and grants from the FBI and Adobe Systems for Hany Farid, both involved in CSTRC. Another research team recently received funding from HSARPA for a new project related to wireless network security, and from I3P for a new project related to SCADA security. We'll describe these new projects in the next issue of the newsletter.



David Kotz,
Executive
Director

Photo: Joe Mahling '69

Clinical experiments begin to support first responders and casualties

A research team in the Emergency Readiness and Response Research Center at ISTS has developed a system of remotely monitoring the physiology of first responders and casualties during emergencies. The system, called ARTEMIS (Automated Remote Triage and Emergency Management Information System), consists of physiological sensors and a computing device with wireless communications to transmit data.

"We are using sensors and developing algorithms to remotely determine physiological condition in the same way that EMS or medics would in person," says ER3C's Director, Sue McGrath. "Our device assesses the subject's airway, breathing and circulatory state, and instead of using a suite of sometimes cumbersome and specialized sensors, we have been focusing on the use of a pulse oximeter, an inexpensive, commercially available device commonly used in hospitals that measures a patient's heart rate and the percent of oxygen in the blood."

While heart rate and oxygen saturation are good indicators of circulatory state and a delayed indicator of respiratory state, the researchers realize that first responders must be able to acquire real time breathing and airway information to successfully perform triage. To achieve this, the researchers have begun clinical studies to analyze the waveform that is produced by the pulse oximeter, called a photoplethysmogram.

Janelle Chang, Thayer M.S. student, Sue McGrath, George Blike (Dartmouth-Hitchcock Medical Center (DHMC) Anesthesiologist), and Metin Akay (Thayer School professor), working with the Sleep Disorders Laboratory at DHMC, have been exploring the features of the photoplethysmograph signal that are predictive of obstructive events, i.e., events that block the airway of a subject. Data was gathered from patients wearing a forehead pulse oximeter during an overnight stay. Preliminary results from this study indicate that there is a change in the photoplethysmograph waveform morphology during obstructive events. The group will next examine data from additional patients and develop algorithms that can automate the detection of obstructive events using the photoplethysmograph generated by the pulse oximeter.



Left to right: Suzanne Wendelken, TH '04, Janelle Chang TH '04, Kirk Shelley, Scientific Chair of the Society of Technology in Anesthesia Conference '05, Miami, FL, January 2005.

Janelle and Suzanne are awarded "Best Clinical Use of Technology" for the poster, "Investigating respiratory variation in the plethysmograph to identify obstructive sleep apnea."

Suzanne Wendelken, research associate at ISTS (Dartmouth Class of '02 and Thayer School of Engineering Class of '04) is conducting another study using photoplethysmograph data. Wendelken has been working with McGrath, Blike and Steve Linder, a visiting professor of computer science, to explore the use of the photoplethysmograph in detecting breathing variations in post-operative patients in the Post Anesthesia Care Unit at DHMC. This signal is influenced both by the cardiac and respiratory cycles. Respiratory-induced variations in photoplethysmograph amplitude have been documented and associated with airway obstruction, hypovolemia, and hypotension.

Wendelken and Linder developed algorithms to extract pulse morphology parameters from the photoplethysmograph using a feature extractor that allows them to obtain statistics about each individual pulse, including pulse height, width, and area, as well as rise and fall time.

"Our experimental results demonstrate that these features show measurable variations due to respiration, can provide a reliable measure of respiration rate, and help protect and care for emergency responders and casualties during emergencies," says Wendelken.

Cyberwarfare Study Cited by World Security Newsletter

Cyberwarfare is a real future threat. That is the conclusion of an ISTS study recently reviewed in the Network World Security Newsletter. The study, titled *Cyberwarfare: An Analysis of the Means and Motivations of Selected Nation States*, is co-authored by Charles Billo, ISTS Senior Researcher, and undergraduate student Welton Chang, class of '05. Their monograph, published by Dartmouth in November 2004, synthesizes current open source data to assess the capabilities and offensive doctrine of selected foreign states with respect to computer attacks against IT networks and other critical economic infrastructure in the U.S. Billo and Chang prepared their study—covering China, India, Iran, North Korea, Pakistan, and Russia—under a grant provided by the Department of Homeland Security.

“Cyberwarfare involves units organized along nation-state boundaries in offensive and defensive operations employing computers to attack other computers,” says Chang. “Hackers and other individuals trained in software programming are the primary executors of these attacks. These individuals often operate under the auspices of nation-state military and related services.”

The authors contend that the Internet today may not be as resilient as some experts believe due to “convergence”—the market-driven progression toward central network hubs that present a potentially lucrative target for hackers. Moreover, the study observes, as advanced industrial states outsource their software programming to countries such as India, Pakistan, China, and Russia, the risk of rogue programmers using their access to commit cyber attacks rises. The possibility of abuse by hackers, organized crime agents, and cyber terrorists grows as more and more programming is subcontracted to those countries for economic reasons.

A copy of the study is available at <http://www.ists.dartmouth.edu/NL/v1/n4/cyberwarfare.html>

I3P News

Knowledge is of two kinds. We know a subject ourselves, or we know where we can find information upon it.

—Samuel Johnson

English author, critic, & lexicographer (1709 - 1784)

While Samuel Johnson could never have anticipated the development of knowledge bases, the above quotation does capture the spirit behind the creation of a new service from the Institute for Information Infrastructure Protection (I3P). The I3P Knowledge Base, while still in its electronic infancy, promises to be a key service I3P provides to Consortium members.

Late in 2003 the Knowledge Base was described as a digital archive that would support the I3P's initial mission to facilitate information sharing and highly effective research among Consortium members. The goal was to have the archive serve as a central repository for electronic preprints of information security research articles, offer tools to analyze and organize cyber security research, and facilitate faster, broader dissemination of the latest research findings to the cyber security community. While certainly a sound plan, there were many challenges associated with amassing prepublication information produced by our membership, and disseminating cyber security research.

A needs assessment, undertaken in the summer of 2003, revealed that Consortium members were interested in a host of services that went beyond the original concept of a digital archive. Consortium members expressed a need for access to funding opportunities in relevant research areas,

a calendar of cyber security events, collaborative work spaces for conducting Consortium business, opportunities for sharing research findings, and access to previously unpublished information. Over the next year the newly formed Knowledge Base team focused on building a service and populating it with quality content. Along the way the Knowledge Base also became the publisher of Security in the News, a highly-used daily cyber security news aggregation service. The close of 2004 saw the I3P with a fully functioning set of information services, but with much work left to be done.

In 2005 there will be a series of enhancements and new features added, including an expanded Members' Space, secure synchronous and asynchronous areas for research teams to work, and a digital repository. Specifically, the repository will be a collection of meta-records, harvested from our Consortium members' collections, and meta-records locally created. The meta-records will conform to national standards, showing not only the standard descriptive information about each information asset contained within the repository, but also how the information may be accessed. In tandem with the repository, Consortium members will be working on developing a taxonomy of cyber security terms.

The I3P Knowledge Base may be accessed at <http://www.thei3p.org>

Distributed honeypots

Mixed with all the urgent, useful, or just plain silly traffic on the Internet is a constant barrage of hazardous cargo: sniper-like hacker attacks, self-propagating automata (“worms”), artery-clogging junk email “spam,” and spam-borne viral infections. ISTS researchers are using honeypots, a tool for monitoring and analyzing Internet traffic, to learn how attackers deploy their hazardous cargo. Honeypots serve as a lure; they are normal computers with the sole purpose of being attacked.

Honeypots are used mainly in open-source development and other security research groups. Because the honeypot's address is unadvertised, and its system provides no production purpose like a mail or web server, nobody has legitimate business with it. Any interaction with a honeypot across the network is considered potentially hostile and is recorded in several ways for later scrutiny.

A principal goal of the current ISTS research is to evaluate the suitability of honeypots for broader use with less required manual analysis and control. To that end, high-fidelity views of honeypot activity, including network sniffer, operating system kernel and filesystem activity logs, are aggregated and presented to an analyst's console for rapid identification of notable malicious activity.

ISTS's honeypots are virtual machines running within a host, one that monitors all the network traffic to and from the honeypot, and much of its internal state. This provides a richer set of activity data and simplifies the administration process. Researchers deploy such systems in a variety of domains, and automatically log their adventures in a centralized database for detailed analysis. These honeypots are distributed to different host sites around the Internet.

To enable monitoring of the probes and attacks on the distributed honeypots, the distributed honeypots team implemented extensions to the User-Mode Linux virtual machine environment. The first (TTY logging) monitors all commands typed by an attacker that has gained entry into the virtual machine, even if the network traffic carrying those commands is encrypted. The extension looks at the commands after the traffic has been decrypted at a choke point in the Linux kernel.

The second extension records all system calls made by applications run inside the virtual machines. Every request made by a running program to the operating system kernel is logged by the honeypot. This includes processes that try to hide their communications through cryptography as well as legitimate programs that are subverted by an attacker. The resulting flood of raw data will provide a good picture of the types of actions going on in the system even by automated tools in the honeypot.

Keeping Goldilocks Out: A Tale of the Bear/Enforcer

Professor Sean Smith, Director of the ISTS's Cyber Security and Trust Research Center, asserts that breakthroughs in secure programming are scarce and will continue to elude interests in both the public and private sector, in spite of recent national attention to cybersecurity, network crippling cyber-crime and fears of a cyber-terror attack. He and his students in Dartmouth's PKI Lab, funded in part by ISTS, believe that part of the solution to more secure computing lies in hardware solutions, particularly in the use of trusted platform modules (TPMs).

John Marchesini, a doctoral student at the PKI Lab explains, "There is little incentive in the private sector to make software more error proof or to test for vulnerabilities, as time-to-market is often the deciding factor in product success, not security." Marchesini has been a leading force behind the Bear/Enforcer project, a kind of system 'chaperone' that makes sure the links your computer makes and the applications it plays with meet accepted security norms set by the system administrator.

The Enforcer is a virtual secure co-processor built on top of Trusted Computing Group hardware. Currently designed for a Linux operating environment, it prevents tampering by detecting deviations in trusted properties of a system, directory or files.

As every file is opened, the Enforcer verifies its integrity given specified administrator security policies and responds in a number of possible ways. Actions designed into Enforcer include "any combination of logging the error, denying access to the file, and parking the system," according to a recent paper from the lab. This allows sensitive data to be protected from an attacker. "It is, to our knowledge, the only freely available software that takes advantage of the trusted platform module in TCG hardware," says Marchesini.

When trusted computing platforms first emerged, they were quickly enveloped in the heated debate about digital rights management that shut down Napster and threatened the future of open source programming. Bear / Enforcer brought balance to the debate by applying the TPM specification to three open-source applications: Apache Web server, OpenCA certification authorities and— with SELinux—compartmentalized attestation. Attestation refers to the ability of one computer to prove to someone or something else that it is in a specific configuration. Attestation can be used to verify that a remote computer fits or violates machine or admin security policy specifications.

In the SELinux application, the Enforcer group was able to in part address the "Big Brother" fears

of the privacy and open-source community by creating a limiting feature of the TPM. A user can verify the validity of a file or program running on another system but only has access to the software compartments relevant to the attestation being performed. Remote systems (like a recording studio looking for pirated music) do not have the ability to search throughout a user's system for violations of the security policy; they are limited to searching in a very specific area. The project results have drawn the interest of such industry players as McAfee, Intel and SAP as well as numerous places in academia.

"We depend on computers and the software they run to do a lot of things: run our cars, run medical equipment, critical infrastructure, everything. Unfortunately, because of bad programming, bad tools and the sheer complexity of software, it is really easy to penetrate machines and their systems," says Marchesini, who has been an author of several papers on Bear/Enforcer, under the direction of Smith.

Smith notes "If we are to progress, we need to make computing secure." Platforms such as Bear/Enforcer may illuminate the path towards a more secure programming future.

For more information please visit <http://enforcer.sourceforge.net>

honeypots continued from page 2

"The logs we collect give us a clear view of the attacker's actions, tools, and in some cases even their motives," says Bill Stearns, Senior Research Engineer. Because of the volume of data gathered by the honeypots, researchers are both using existing analysis tools and developing tools specifically for this project. The ISTS work allows the researchers to drill down into individual packet payloads, watch for trends and reassemble any software that has been up/downloaded by the attacker.

All of the tools and extensions developed during this project will be available through the ISTS website or can be requested by emailing honeypots@ists.dartmouth.edu.

Discovering attack methods

It's 10:22pm in Bucharest, and our attacker has already left the cybercafe for the evening. Before heading out, he started up his scanner, running remotely on a compromised Linux machine in Irvine, Ca., then logged out of the shared pc. The scanner is looking for old versions of the Washington University FTP server, wu-ftpd. When it stumbles across our honeypot, it immediately launches a pre-scripted attack and keeps on scanning. In the 2.11 seconds between first probing, then attacking our honeypot, it has attempted over 1600 connections to other systems.

The attack is old, but effective - a heap corruption exploit - leaving behind a root shell for the new owner.

10:33am the following morning, danielo (one of the account names he uses), stopped by the cafe and checked his tool's progress. He didn't have much time, so he quickly instrumented the machine with several new accounts and backdoors, and he installed not one, but three rootkits, redundantly making a mess of the system. Interestingly, danielo didn't see the need (or wasn't experienced enough) for much customization or personalization of his tools. One such two-year old script tried feebly to email a log of its "successes" to a yahoo account; I highly doubt this is still a viable maildrop. Danielo is early in his cracking career.

2:53pm he's back, learning how to install tools, failing repeatedly to access files he placed in the ftp server filesystem, and gaining experience for future exploits. While danielo's skills are limited, his tenacity is notable. It is quite likely that his unrefined methods are sufficient to build a formidable stable of rootshells for sale, rent, or just plain entertainment.



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@ist.s.dartmouth.edu

www: ist.s.dartmouth.edu

Announcements

Sean Smith receives NSF CAREER award



Assistant Professor of Computer Science Sean Smith has received the prestigious National Science Foundation CAREER award. The CAREER program recognizes and supports the early career-development

activities of those teacher-scholars who are most likely to become the academic leaders of the 21st century. He is studying how to use public key infrastructure (cryptographic tools for identity and information integrity) and trusted computing technology (hardware tools for computational integrity) to build trustworthy relationships among users spanning many organizations. The NSF CAREER Award will aid Smith in his work to bridge the gap between current information infrastructure technology and the trust requirements that people have. ISTS applauds Sean's efforts in cyber security.

Hany Farid receives FBI grant and Adobe gift



Photo: Joe Merling '89

The FBI awarded Hany Farid, Associate Professor of Computer Science, a grant that will allow him to hire professional programmers to turn his image-tampering software, currently in prototype form, into a more complete tool.

The FBI needs such tools for their analysis of photographic evidence.

Adobe Corporation, best known for its Photoshop product, has also donated funds to Farid's lab. Adobe hopes to incorporate some of Farid's work on digital image forensics into a new product and possibly into Photoshop.

Farid's image-tampering work is partly funded by ISTS and has many applications.

ISTS External Advisory Committee

This new committee will meet two or three times per year, advise ISTS leadership, and report back to the Provost.

The committee members are:

Professor Farnam Jahanian - Professor of EECS, University of Michigan and Founder of Arbor Networks.

Professor Bobby Schnabel - Associate Vice Chancellor for Academic and Campus Technology, University of Colorado at Boulder.

Myra Socher - Adjunct Assistant Professor of Emergency Medicine, The George Washington University School of Medicine and Health Sciences and Adjunct Instructor in Nursing (Health Systems Management), Vanderbilt University School of Nursing.

Professor Jeannette Wing - President's Professor of Computer Sciences and Department Head, Carnegie Mellon University.

ISTS thanks them for their willingness to advise us as we pursue our mission.