

## From Our Director



Photo: Joe Mehling '09

David Kotz

In addition to the many interesting articles in this issue, I wanted to point out two new exciting developments here at ISTS.

First, Dartmouth's Interactive Media Laboratory recently launched a new, video game-based training program for first responders featuring simulated terrorist attacks using weapons of mass destruction. The program, called "Ops-Plus for WMD Hazmat," is the first course for the Virtual Terrorism Response Academy (VTRA). The course provides more than 16 hours of training to handle CBRNE (chemical, biological, radiological, nuclear, and explosive) emergencies. VTRA was funded by ISTS under DOJ and DHS support.

Second, we are pleased to welcome Tom Candon to ISTS as our new Associate Director. He arrives at ISTS after ten years with Science Applications International Corporation (SAIC) in Washington, DC, where he was Assistant Vice President and Assistant Division Manager in the Advanced Systems & Concepts Operation. Tom was a program manager on three research and development projects focused on improving the analysis process and information sharing within the Intelligence Community by applying software toolsets to operational problems. Prior to his work in the Intelligence Community, Tom was a project director in SAIC's Strategic Assessment Center. While there, he conducted research on a number of topics including organizational adaptation and emergence for the defense department, organizational, policy, and doctrinal issues related to information operations and Homeland Security for the Joint Chiefs of Staff, and the Revolution in Military Affairs for the Office of the Secretary of Defense. Before joining SAIC, Tom worked as a research assistant at the Industrial College of the Armed Forces within the National Defense University.

Finally, ISTS research has received a lot of attention in the press of late. Our work on "virtual walls," an abstraction to allow everyday users to manage their privacy in tomorrow's sensor-rich world, received Honorable Mention for Best Paper at Pervasive 2007, and then was written up in several newspapers. Our work on the risks large enterprises face when employees use peer-to-peer file sharing systems, sometimes exposing sensitive company information, was also covered in several newspapers. You can find links to all this news, and other relevant information, on our web site.

## Building the Security-to-Business Bridge

The Center for Digital Strategies at the Tuck School of Business at Dartmouth College and Tuck Executive Education are organizing a pilot management education program for corporate information security professionals entitled "Building the Security-to-Business Bridge." The course is funded as part of an ISTS award from the National Cyber Security Division (NCSA) of the Department of Homeland Security.

An important part of ensuring our national security is the security of the nation's critical infrastructures, including the business organizations that compose them. It is often up to the information security professionals in these companies to help guide corporate leadership to make changes. However, many of these security professionals find their security initiatives hindered because of their inability to communicate effectively within the business.

"Understanding the technology and the technical risks is simply not enough to generate action," says Hans Brechbühl, executive director of the Center for Digital Strategies and an ISTS faculty affiliate. "A deeper understanding of the business, the overall risks it faces and how investment decisions are made is crucial."

The communication failure often stems from an underlying lack of business education, a lack of understanding of how to change the corporate culture around security, and an inability to communicate the business case for information security.

Tuck's pilot program will enhance the skills information security professionals need to address corporate information security challenges in terms that their business colleagues and senior corporate executives will more readily understand.

The program will be developed in conjunction with leading CISOs (Corporate Information Security Officers) from Fortune 500 firms. The course will convey business concepts and skills that will help the information security professional to better understand how business leaders think, appreciate organizational dynamics, build an information security strategy, and create a business case for security investments.

"While this program will certainly have a significant impact on the practice of security management," says Eric Johnson, the Center's director and Tuck professor, "we believe it will also represent leading-edge education and be a power-

### In This Issue

Wi-Fi Wireless Network.....	page 2
Rebuilding Confidence.....	page 2
Ensuring Data Authenticity.....	page 3
Congratulations Grads.....	page 3
Information Risk in the Professional Services.....	page 4
New Publications.....	page 5

Continued from page 1

ful way to bring top information security professionals into the research process at Dartmouth—bringing theory and practice of information security closer together.”

The program leaders envision a three- to three-and-a-half-day program for up to fifty participants. Possible session topics include: “Strategic Mindset and Strategic Planning”; “Organization Structure and Culture”; “Brand Management and Protection”; “Using a Financial Model to Make the Business Case for Security”; and “Corporate Governance”. The current timetable is to deliver the pilot program in 2008.

For more information about this program, contact the Center for Digital Strategies at 603-646-0899 or visit the Center website at [www.tuck.dartmouth.edu/digitalstrategies](http://www.tuck.dartmouth.edu/digitalstrategies).



## Judging Wi-Fi Cards by Their Handshakes: Active Fingerprinting of Wireless Devices

Wi-Fi wireless networking (also known as IEEE 802.11b/g), free or commercial, has become an expected feature of any modern public facility. Traveling businessmen hardly think twice about taking out their laptops and trying to connect to the local wireless service provider’s AP, either to use a VPN to their corporate network, or to check personal e-mail.

Shaping these expectations is the ease of use that the users came to associate with wired networks: a typical client computer “just works” once plugged into a wall socket, acquiring a dynamic IP address and other necessary information for full Internet routing automatically. The technical challenges posed by the different physical layer of a wireless network are hidden from the user by design — more or less successfully. This ease, however, does not mean comparable security.

Part of the problem is that the radio medium is typically shared between a number of networks controlled by independent organizations, while a wall socket is controlled by the physical owner of the brick-and-mortar building; others are due to the fact that the 802.11 standard was developed by a consortium of vendors, trying to accommodate all sorts of future developments envisioned by the participating parties. The result is the so-called “design by committee”, known to complicate the specification by, at least, an order of magnitude.

## Rebuilding Confidence

*Humanitarian organizations, donor relationships, and digital strategies*

Humanitarian organizations address great suffering in the world, channeling aid from wealthier, more developed countries to victims in every corner of the globe. While the heroic efforts of these organizations are widely admired, visible response failures to recent large disasters have shaken the confidence of donors and the general public. This has led traditional donors—individuals and governmental organizations—to express disappointment in the operational performance of humanitarian organizations and in the humanitarian sector as a whole.

The question facing humanitarian executives is how to restore confidence, in particular the confidence of large-scale governmental donors who work with them as long-term partners and provide the bulk of the funding. As the sector has begun to come to grips with this issue, two directions for improvement have emerged.

The first is to create more effective organizational structures with clear chains of command and clear demarcation of decision-making authority and responsibility. This direction comes out of the Hurricane Katrina response experience. The second is to improve information management and decision-making processes in the area of supply chain management—the management of the set of activities necessary to specify, procure, transport, store, and distribute relief items. Key to this second area is much greater use of information technology (IT) and information systems that leverage and mimic technology that has long been in use in the commercial world.

The Center for Digital Strategies at the Tuck School of Business is conducting research that explores how issues of trust, control, and confidence in partner cooperation have come into play in setting IT direction for humanitarian supply chains. Working with a leading humanitarian organization, the Center is examining how IT is currently used to provide control and build trust within the supply chain, and to assess how well existing theory on trust and control applies in the humanitarian setting. They have found that, while control is difficult to implement due to lack of goal alignment and task complexity, it has the advantage of being hierarchical. That is, control mechanisms implemented between the home office and country offices to build confidence also build confidence between parties in the next supply chain echelon—between donors and the humanitarian organization.

To learn more about the Center and its research on IT implementation to enable humanitarian relief, visit our web site: [www.tuck.dartmouth.edu/digitalstrategies](http://www.tuck.dartmouth.edu/digitalstrategies), and look under Research Projects.

TUCK SCHOOL OF BUSINESS AT DARTMOUTH



GLASSMEYER/McNAMEE  
CENTER FOR  
DIGITAL STRATEGIES

Continued on page 5

# Ensuring Data Authenticity in Internet-based Computing

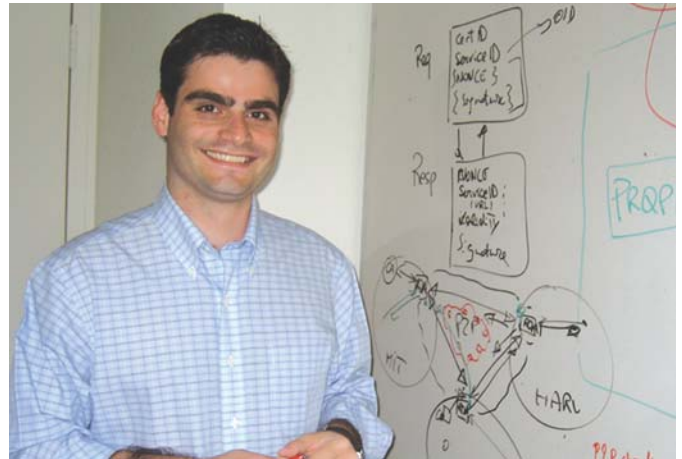
by Nikos Triandopoulos

With the advancement of networking technologies and the development of fast web-scale protocols for distributed data management, a growing number of applications are realized "in the cloud": they operate in a model where storing and computing resources are provided by remote servers or unknown devices. For example, data-storage systems built over P2P networks, file systems outsourced to networked storage units or Internet-based storage used by web applications, all provide end-users with a virtual view that everything runs locally, nevertheless data management and computations are executed remotely, generally by untrusted machines. In these distributed and potentially hostile computing environments, authenticating data and results of computations is necessary in order to ensure the integrity and trustworthiness of any application, especially given the current trend in modern system design towards decentralized architectures with minimal trust assumptions.

In an I3P-funded project we address this problem, by designing lightweight protocols that augment the communication between data sources and data outsourcers to provide secure verification mechanisms for data authenticity and reliable system functionality. In particular, our data authentication protocols allow a client to outsource data storage to a server, ask the server to perform a series of operations on the data and, after the execution of each operation, verify that the operation was executed correctly, in consistency with the history of previous operations. Each operation is either a query that retrieves data items or an update that adds, removes, or modifies data items. Upon receiving the result of a query operation, the client can easily check the integrity and completeness of the data returned. By employing elaborate algorithmic and low-cost cryptographic techniques, we achieve high levels of efficiency without compromising security: the client maintains some minimal state and verifies operations in real time; the server maintains an efficiently stored and managed collection of carefully computed data digests that assist the client's verification task.

The above patent-pending technologies serve as a general-purpose authentication tool, designed to be platform-independent as well as agnostic of the implementation details of applications or storage components. In particular, the storage server could be as large as a network service provider, as complex as a P2P network or as small as a USB drive. Likewise, stored data can be as simple as a collection of files indexed by keys and unstructured data objects or as complex as hierarchically organized data (e.g., file systems or XML documents); analogously, the authenticated functionality

ranges from basic dictionary operations to complex file-system operations. Overall, these technologies provide a transparent security layer between applications running on a local machine and data stored elsewhere that ensure that all data used is trustworthy and reliable.



Nikos Triandopoulos is a Research Fellow at ISTS. He earned his PhD in Computer Science at Brown specializing in secure protocol design for data authentication. His current research focuses on secure distributed data management and security and privacy in peer-to-peer and sensor networks, on which he collaborates with the members of DEVLAB and MetroSec at Dartmouth and Center for Geometric Computing (CGC) at Brown.

## Congratulations to ISTS-involved students that graduated this spring with theses or dissertations

*Devin Brande, MS, "Estimation of Tire Forces for a Differential-Steered Robot".*

*Wayne Chung, Ph.D, "Dynamic Social Network Analysis".*

*Nihal D'Cunha, MS, "Exploring the Integration of Memory Management and Trusted Computing".*

*Andrew Flynn, BA, "WikiD: Dartmouth Wiki Implementing Fine-Grained, Decentralized Access Control".*

*Annarita Giani, PhD, "Detection of Attacks on Cognitive Channels".*

*James Joslin, MS, "The design, construction, and control of the DynaBot testbed".*

*Glenn Nofsinger, PhD, "Plume Tracking in Sensor Networks".*

*Kevin Olds, AB, "Wheel-Terrain Pressure Distribution Data Acquisition for Small Mobile Robots".*

*Anthony Portera, MBA, Worked on the "Information Risk in Professional Services (IRIPS)" project.*

*Yong Sheng, PhD, "The Theory of Trackability and Robustness for Process Detection".*

*Evan Sparks, BA, "A Security Assessment of Trusted Platform Modules".*

*Sheng Zhang, Ph.D, "Building Trustworthy Recommender Systems".*

*Wei Zhang, MS, "Automatic Ontology-Based Indexing".*

# ISTS Embeds Students in Financial Institutions

by Tony Portera T'07

The Tuck curriculum allows for students to take the month of December to focus on projects and activities of their own choosing. I took the opportunity to join the Information Risk in the Professional Services (IRIPS) team on a Financial Institution Field Study. The field study gave me the chance to team up with Computer Science Ph.D. candidate, Sara Sinclair, as we set up shop in Manhattan to interview a number of information security professionals. While she focused on technical details and design initiatives, I sought to investigate the organizational dynamics driving security innovation and how innovation can be fostered in an area focused on protecting others from risk.

Organizations often see information security as corporate overhead, not a source of value creation or a competitive advantage. By its nature, security often focuses on closing barn doors *after* a breach. Many security professionals who cut their teeth in law enforcement are steeped in staying inside the lines; checking the boxes; making sure that everything is by the book. But with the threats ever evolving, cyber security requires innovation to stay ahead. Some Chief Information Security Officers (CISOs) wishfully look outside hoping to buy innovation. Others are looking inside their own organizations, hoping to jump start the innovation engine.

Of any industry, financial services face the most creative and seemingly endless parade of threats. The significant potential rewards keep thieves working overtime to exploit any weakness. Coupled with large and complex organizations that are constantly innovating with new products and go-to-market strategies, protecting information requires innovative security organizations.

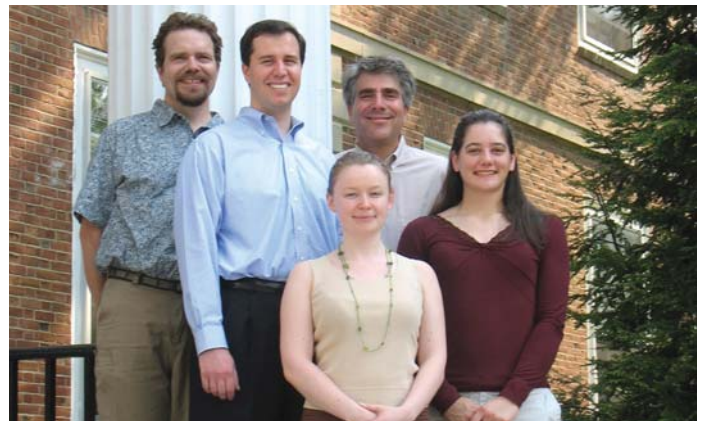
One of the organizations we profiled stood out for its excellence in innovation. Like their competitors, they had a "whatever it takes" mandate to protect firm systems. However, this firm took the mandate and turned it into a mantra. Many of the professionals who join the team bring backgrounds in various technical and non-technical fields but not security. They learn security on the job and are expected to be fluent in both the IT needs and the business activities of the firm. When they discover a need to mitigate risk they do not give the task to another organization - rather team members develop their own solution, leveraging external vendors and/or developing a solution using resources from its technology group.

As part of my work in the team, I helped identify what made this firm's security organization extraordinary. Much of their success stems from their culture of anticipating and mitigating risk supplemented with a thoughtful organizational design. Embedded in this successful organization is a:

- pairing of risk mitigation design and development
- commoditization of risk mitigation strategies – develop, make simple, pass on administration, retain thought ownership
- dedication to building the firm reputation
- openness to collaboration

This project has forever changed my view of how information security is a topic that current and future managers cannot just assign a budget to and hope it goes away. It is an area that requires understanding organizational needs and fostering of a culture to engage and innovate on those needs. Whether the organization is of a small size and needs to be simply thoughtful about the packages it buys or is large enough that building custom solutions is an option, cultural pride, discipline and openness to collaboration are necessary to mitigate risk appropriately.

My IRIPS field study gave me a fascinating, in-depth view into the technical activities of the world's leading financial institutions, a chance to participate in the field of academic research and the opportunity to work more closely with a professor that I had grown to respect in the classroom. It was a great way to spend my winter break and I feel it has enriched my perspective as a future manager.



*IRIPS Team*

*From left to right: Prof. Sean Smith, Tony Portera, Prof. Eric Johnson, Sara Sinclair, Stephanie Trudeau*

## Kudos

Congratulations to Professors Fillia Makedon and Jamie Ford (ISTS Affiliates, now of UT Arlington) and Matt Bishop (UC Davis) received \$500k for a three-year NSF Cyber Trust project entitled "Collaborative Research: Detecting and Preventing Attacks in Recommendation Systems."

Continued from page 2

Unfortunately, more software complexity almost invariably means more vulnerabilities. Additionally, wireless device drivers are a relatively recent addition to the OS kernels, their developers pressured by customer demand. Yet, unlike other drivers, they are directly exposed to whatever malicious inputs an attacker might throw at them. Disabling unnecessary network services has become the security rule of thumb; alas, disabling unused wireless features is typically not an option, leaving the users vulnerable.

The point was driven home last year by security researchers John Ellch and David Maynor, who produced an exploit for Mac OS X wireless drivers that gave the attacker full control of a laptop as soon as it was opened up (with the wireless interface enabled), at the deepest OS level. The flaws were not limited to Mac OS: Windows proved just as vulnerable.

The ISTS fingerprinting project is aimed at both detecting vulnerable wireless devices and exposing their weaknesses arising from the vendors' deviations from the IEEE 802.11 standards. In our controlled environment, a specially configured "attacker" platform unleashes a stream of malformed traffic at a target device, and observes the responses that might indicate a possible vulnerability or a deviation of the standard. Such responses are learned and catalogued, the approach known as "active fingerprinting".

The accumulated information can be used to detect known vulnerable combinations of drivers, firmware and hardware, in order to warn the owners, and to prevent the vulnerable platforms from endangering the network to which they are attempting to connect. The information derived from this project will be useful to the larger MAP (Measure-Analyze-Protect) wireless effort at Dartmouth.

### **New Research Project supported by the Bureau of Justice Assistance (BJA)**

#### **DIST Visualization Experiments (DIST-Vis)**

*Fabio Pellacini, George Cybenko*

The Dartmouth Internet Security Testbed (DIST) project extracts large volumes of real-time network data from various campus network instrumentation points. Monitoring network events is expected to reveal trends in network traffic that would eventually lead to the detection of a wide range of network attacks, novel business processes and network performance trends. This collaborative project seeks to develop novel techniques for visualizing human processes as overlays on the physical network topology, and for displaying deviations of behaviors from modeled behaviors so that analysts can better understand how behaviors are drifting over time, whether sequences of deviations are random fluctuations or meaningful trends.

## **New Publications**

Laura Kopczak, M. Eric Johnson, "Rebuilding Confidence: Trust, Control and Information Technology in Humanitarian Supply Chains"; Proceedings of the Academy of Management Annual Meeting, Philadelphia, PA, August 3-8, 2007.

W. Wang and H. Farid, "Exposing Digital Forgeries in Interlaced and De-Interlaced Video"; IEEE Transactions on Information Forensics and Security, 2007.

Yi Ouyang, Zhengyi Le, Yurong Xu, Nikos Triandopoulos, Sheng Zhang, James Ford and Fillia Makedon, "Providing Anonymity in Wireless Sensor Networks". In Proceedings of the IEEE International Conference on Pervasive Services (ICPS), Istanbul, Turkey, July 2007.

Roberto Tamassia and Nikos Triandopoulos, "Efficient Content Authentication in Peer-to-Peer Networks". In Proceedings of the International Conference on Applied Cryptography and Network Security (ACNS), LNCS, Volume 4521, Springer-Verlag, pp. 354-372, Zhuhai, China, June 2007.

Massimiliano Pala and Sean W. Smith, "AutoPKI: a PKI Resources Discovery System"; EuroPKI-2007 - 4th European PKI Workshop: Theory and Practice, Mallorca, Balearic Island, Spain, June 28-30, 2007.

Peter C. Johnson, Apu Kapadia, Patrick P. Tsang, and Sean W. Smith, "Nymble: Anonymous IP-Address Blocking," The 7th Workshop on Privacy Enhancing Technologies (PET '07), Ottawa, Canada, June 20 - 22, 2007.

Apu Kapadia, Prasad Naldurg, and Roy H. Campbell, "Distributed Enforcement of Unlinkability Policies: Looking Beyond the Chinese Wall," IEEE Workshop on Policies for Distributed Systems and Networks (POLICY '07), Bologna, Italy, June 13 - 15, 2007.

H Farid, "Digital Doctoring: Can We Trust Photographs?"; In Deception: Methods, Motives, Contexts and Consequences, 2007.

M Johnson and H Farid, "Exposing Digital Forgeries Through Specular Highlights on the Eye "; 9th International Workshop on Information Hiding, Saint Malo, France, June 11-13, 2007.

Ming Li and David Kotz, "Group-aware Stream Filtering"; Proceedings of the Fourth Workshop on Wireless Ad hoc and Sensor Networks (WWASN), Toronto, ON, Canada, June 25, 2007.

Apu Kapadia, Tristan Henderson, Jeffrey Fielding, and David Kotz, "Virtual Walls: Protecting Digital Privacy in Pervasive Environments," The Fifth International Conference on Pervasive Computing (Pervasive '07), May 13 - 16, 2007. C Springer-Verlag.

Apu Kapadia, Patrick P. Tsang and Sean W. Smith, "Attribute-Based Publishing with Hidden Credentials and Hidden Policies," The 14th Annual Network & Distributed System Security Symposium (NDSS '07), San Diego, CA, February 28 - March 2, 2007.

Institute for Security Technology Studies at Dartmouth  
 (Interdisciplinary research and education for cyber security and trust)  
 45 Lyme Road  
 Hanover, NH 03755-1219  
 phone: (603) 646-0700  
 fax: (603) 646-0660  
 email: info@ists.dartmouth.edu  
 www.ists.dartmouth.edu

## Past Speakers

May 14, 2007  
**"The Challenges of Storage System Growth"**  
 A talk by Denis Serenyi, Senior Research Engineer, Symantec Research Labs.



May 8, 2007  
**"Deception in Defense of Computer Systems"**  
 A talk by Neil C. Rowe, Center for Information Security Research, Computer Science Department U.S. Naval Postgraduate School



May 1, 2007  
**"New Systems Challenges in the Multi-Core world"**  
 A talk by Dr. Raj Yavatkar, Intel Fellow.



April 26, 2007  
**"Secure Sensor Network Aggregation and Detection of Replicated Nodes"**  
 A talk by Dr. Adrian Perrig, Carnegie Mellon University.



April 20, 2007  
**"Building Shared Reference Monitor Systems"**  
 A talk by Trent Jaeger, Pennsylvania State University



March 29, 2007  
**"A Socio-Technical Perspective on Internet Security: Why the Problem is Even Harder Than We Think"**  
 A talk by Dr. David Clark, Senior Research Scientist, MIT.



## Upcoming Fall Speakers

**October 18th**  
 Dr. Ming-Yuh Huang  
 Program Manager - Strategic Information Assurance R&D, Boeing

**November 6th**  
 Dr. Carl Landwehr, Sr Research Scientist, Institute for Systems Research

**November 15th**  
 Dr. Pamela Samuelson, Professor, School of Information, Univ. of California at Berkeley

### INFORMATION:

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

### CONTACT:

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

Telephone: 603-646-0700

Fax: 603-646-0660