Dartmouth researchers say that PQS is the best approach

Dartmouth engineers George Cybenko and Vincent Berk think that PQS, or process query systems, are the way to go to make sense of the huge volume of data we collect each day from computer network monitors, video surveillance cameras, financial transaction records, databases of email exchanges, etc. The duo present their case in a paper published in this month’s IEEE Computer, the flagship magazine of the Institute of Electrical and Electronics Engineers’ Computer Society.

“PQS closes the gap between gathering a tremendous amount of valuable data and figuring out what the data means,” says Cybenko, the Dorothy and Walter Gramm Professor of Engineering at Dartmouth’s Thayer School of Engineering.

PQS has been an evolving algorithmic and software framework for the past few years. Cybenko and Berk say that PQS is a useful and incredibly powerful tool to quickly analyze credit reports for ID theft, discover attacks on computer networks, and measure activity at, say, national borders, mall parking lots, or wildlife refuge areas. According to Cybenko, “PQS can do for discrete, categorical data analysis problems what classical times series analysis did for finance and control systems where the data are numerical.”

It is based on the premise that sensed environments, be they computer networks, email traffic, or high-security buildings, all consist of processes with distinct states, dynamics, and observables. PQS works to detect and understand the changes or irregularities in these processes. The PQS software is easily installed with the sensor equipment to collect, monitor, and sort out a great deal of data.

“I think the most interesting application of PQS to date is in network security monitoring,” says Vincent Berk, research associate and lecturer at Dartmouth’s Thayer School. “Network administrators have many options when it comes to monitoring tools, but none of them are integrated; and, while

Finding Patterns of Importance in a Deluge of Data

Continued on next page
all of them produce useful information, it’s often in hugely impractical quantities. PQS brings together the information, and effectively focuses on the most important issues first. To my knowledge there has not been a new software technology that is this versatile since the introduction of relational databases.”

This work is a project of Dartmouth’s Institute for Security Technology Studies, and is supported in part by funding from the US Department of Homeland Security (Science and Technology Directorate), and the Department of Defense (DTO, AFRL, and DARPA).

**ISTS to Host I3P Consortium**

On March 21st and 22nd, ISTS will host the Institute for Information Infrastructure Protection (I3P) at Dartmouth. Members of the consortium regularly host meetings to further the organization’s goals to address research and policy-related aspects of the vulnerabilities inherent in the information infrastructure. The I3P is a national consortium of leading university, national laboratories and non-profit institutions dedicated to strengthening the cyber infrastructure of the United States through its various initiatives. These meetings bring experts together to identify and mitigate threats aimed at the U.S. information infrastructure, and promote collaboration and information sharing among academia, industry and government.

The I3P currently supports initiatives in two major areas, one project focusing on the vulnerabilities of supervisory control and data acquisition (SCADA) and other control systems in the oil and gas industry and the second project that explores the business rationale for cyber security, including important policy, risk and economic issues.

For more information about the I3P visit their website at www.i3p.org.

---

**Consumer Data Use Requires Responsibility and Transparency**

Top executives from Facebook, Starwood Hotels Worldwide, Time Warner Cable, and Yahoo! came together at Dartmouth’s Tuck School of Business on January 10 to participate in a panel discussing best practices for collecting, managing, using, and protecting consumer data. The panel concluded a half-day of programs hosted by the Center for Digital Strategies as part of the Tech@Tuck event, “Managing Consumer Data: Improving Service and Protecting Privacy,” presented in collaboration with Dartmouth’s Hopkins Center for the Arts and the Dartmouth Centers Forum.

Professor John Marshall moderated the panel, which began with a discussion of the customer data revolution. He questioned panelists on customer fears and expectations, challenges facing their companies today, privacy issues, and how each company measures success. When asked about customer expectations around personal data exchange, panelists observed that some customers show more willingness to give quality data if they feel they will receive benefits in return.

Anke Audenaert, vice president of content optimization at Yahoo!, described how Yahoo! uses collected data to tailor information presented to a user on the website based on past use of the site. Amy Weinberg, vice president of customer insight at Starwood Hotels Worldwide, commented that hotel guests are delighted when employees are able to recognize them by name and accommodate them based on previously indicated preferences.

All panelists stressed the importance of continuously communicating with customers to discover what customers want. They agreed that companies must be upfront about how customer information will be used. “It’s all about trust,” Chris Kelly, vice president and chief privacy officer at Facebook, said.

The panel participants said they would like to find the balance between active and passive personalization of customer data. The biggest challenge they face today lies in the quality and quantity of data. With 800 to 1.1 billion page views a day, Kelly said it is easy to be overwhelmed by the amount of data available on Facebook. The challenge is in extracting from that data and deciphering what it means to the organization.

Continued on page 4
Virtual Walls: Protecting Digital Privacy in Pervasive Environments

As pervasive environments become more commonplace, the privacy of users is placed at increased risk. The numerous and diverse sensors in these environments can record a user’s activities and personal information such as heart rate, body temperature, and even conversations. Users may unwittingly leave “digital footprints” (information about users derived from sensors) that can threaten their privacy and must thus be allowed to control how their digital footprints are reported to third parties.

While a significant amount of prior work has focused on location privacy, location is only one type of footprint. As the number and variety of sensors grows, it will be cumbersome for users to specify fine-grained policies about a multitude of footprints. To this end, we propose a policy language based on the metaphor of physical walls, and posit that users will find this abstraction to be an intuitive way to control access to their digital footprints. For example, users understand the privacy implications of meeting in a room enclosed by physical walls. By allowing users to deploy “virtual walls,” they can control the privacy of their digital footprints much in the same way they control their privacy in the physical world. Virtual walls can be configured with three levels of transparency that correspond to intuitive levels of privacy — transparent, translucent, and opaque. For example, a translucent wall allows the reporting of general footprints such as room occupancy and temperature, but prevents access to personal footprints. To allow users to better control their privacy, we extend this metaphor by allowing users to create different virtual walls for different queriers. For example, Alice can create a transparent wall around her dorm room that applies to her family and a translucent wall that applies to her professors.

Our goal was to provide users with a usable method for protecting their privacy in pervasive environments. We evaluated the virtual walls model with a user study, and the results indicate that our model is easy to understand and use. This work will be presented at the Fifth International Conference of Pervasive Computing in Toronto, Canada (Pervasive 2007).

ISTS Team Demonstrates “MAP” System to Air Force and Navy

At the invitation of the Air Force Information Operations Center, and coordinated by HSARPA in the Department of Homeland Security, the MAP team took their demo on their road. The MAP project — “Measure, Analyze, Protect” aims to detect and respond to attacks on a production Wi-Fi wireless network on an enterprise scale. Since the MAP system is currently deployed throughout Sudikoff Lab for Computer Science, involving 20 wireless access points and two rack-mounted servers, it was no easy feat to make the demo portable! In the end, six laptops, four access points, and countless cables and accessories were shipped to San Antonio and set up at the host site — the Southwest Research Institute. Key researchers from the Air Force Information Operations Center, and guests from the Naval Research Lab (in Washington, DC) attended. This demo was possible because of the tireless efforts of Yong Sheng, Keren Tan, Bennet Vance, and Udayan Deshpande. In February, the MAP team hit the road again, to demonstrate MAP to the US Secret Service in Miami, Florida.

ISTS Speaker Series

Monday, January 15, 2007
"PKI Implementation"
A talk by Dr. Peter Alterman, Chair, Federal PKI Policy Authority.

Monday, March 12, 2007
"Robust and Predictable Network Anomaly Detectors"
A talk by Dr. Greg Shannon, Chief Scientist, CounterStorm, Inc.
Professor Hany Farid spoke in December at the Project Safe Childhood Conference about his work on Digital Image Forensics and its application to photographic evidence in child pornography in Washington, DC. Project Safe Childhood was launched by the Attorney General earlier this year and has been a high priority for the Department of Justice and all US Attorney offices across the country. The ICAC Task Force and the National Center for Missing and Exploited Children are also partners for this initiative and 800 attendees from across the country attended.

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

Continued from page 2

Concluding the panel, Marshall raised the topic of regulation. In the European environment, there is an assumption that the exchange and use of personal data is a human rights issue, heavily legislated and regulated. In the U.S., it's currently much more patchwork and seen as a commercial transaction. Marshall asked panelists whether the U.S. should regulate more, companies should self-regulate better, or the end-customer should be responsible for knowing who they're interacting with and what their policies are. The group predicted that the U.S. will increase regulation and reflect a mainstream consumer view around the use of personal data. "If there is regulation, it should be a level playing field," stated Craig Goldberg, chief privacy officer at Time Warner Cable.

From left to right, Rebecca Gillan and Amy Weinberg from Starwood Hotels & Worldwide Resorts, Chris Kelly from Facebook, Craig Goldberg from Time Warner Cable, Anke Audenaert from Yahoo!, and John Marshall (moderator).