Phinney on Open Source at OpenHatch

Parker Phinney ’12 was the first recipient of the ISTS-Neukom Institute internship grant. During the Winter 2010 term, Parker interned at OpenHatch in Philadelphia, Pennsylvania. Here Parker fills us in on what he has been doing.

During the winter term, I joined OpenHatch’s modest two-person staff of co-founders Asheesh Laroia and Raphael “Raffi” Krut-Landau. OpenHatch.org is a community website which aims to help the development of free and open source software.

Our working style at OpenHatch is a little unorthodox. We use pair programming, an Extreme Programming methodology where two people share a computer and work together. One person “drives” (does the typing) and the other “navigates.” The idea behind pair programming isn’t necessarily that you trade off - the goal is to best use each person’s skills so the team moves as quickly as possible. We tend to favor having the person who is least familiar with the code sitting in the driver’s seat, at least initially. This way, it’s much more likely that he will be engaged and contribute to the process, whereas if he were just navigating he might feel lost and not want to interrupt. Ideally both people in the “pair” are sitting close together and can share control well.

I usually pair with Raffi, and I usually drive. At first, pairing with Raffi felt like personal training, and I was learning extremely rapidly. Now that I’ve been brought up to speed, pairing with Raffi feels more like a collaborative process. I’ve learned that the most important part of programming is making choices, and Raffi and I build off of each other to choose the best approach to solving a problem. We also help each other catch typos.

Dartmouth Researchers Help Secure the Power Grid

Dartmouth Computer Science Professor Sean Smith with his students and research staff are part of the national Trustworthy Cyber Infrastructure for the Power Grid (TCIPG) team that has been awarded a five-year $18.8 million grant from the U.S. Department of Energy with contributions from the U.S. Department of Homeland Security. This represents continued funding that started in 2005 with funding from the National Science Foundation.

TCIPG will explore the “Smarter Grid,” secure and reliable technology involved in the underpinnings of the nation’s electrical power infrastructure. As power grids are upgraded and connected to online systems to increase efficiency, they become vulnerable to malicious attacks and hackers. The TCIPG team will develop cyber security tools and technologies to ensure that power supplies are not disrupted.

“Power is the critical infrastructure that underlies all other critical infrastructure; if there’s no electricity, we can’t power the Internet, or telephones, or medical equipment,” says Sean Smith, an associate professor of computer science. He is also affiliated with the Institute for Security, Technology, and Society. “It’s great to make a contribution to the effort to secure the power grid. And, because we involve undergraduate and graduate students, and high school students, too, the work furthers our educational mission. The students all get real-world experience and make real-world contributions.”

TCIPG also includes researchers with the Information Trust Institute at the University of Illinois at Urbana-Champaign, the University of California at Davis, and Washington State University, with central coordination of the project at Illinois. The director of the project is William Sanders, a professor in the Electrical and Computer Engineering Department at the University of Illinois at Urbana-Champaign. Many of the researchers in this project, including Smith, are also associated with the Institute for Information Infrastructure Protection, a 27-member consortium of national cyber security researchers.
right now, the focus within OpenHatch is on getting the word about Free/Open Source Software and we believe that it's missing.

We work out of the living room of Asheesh and Raffi's cozy West Philadelphia apartment. I feel like a member of the team here, not just an intern. My input really is valued, and it has even caused significant changes in direction. Despite Asheesh's and Raffi's hesitation, I insisted early on that we focus our energy on building a map to allow users to find open-sourcers near them. Now, a few weeks later, that map (https://openhatch.org/people/) has become the center of a large chunk of our website's functionality.

While our workflow is Extreme, our lifestyle is simple. When lunchtime rolls around, we move to the kitchen where we all “pair” on cooking. Sometimes one or two people bike to the nearby produce trucks to pick up groceries. Our meals are always vegetarian (which I like) and often have a spicy Indian flair. Oh, and we also pair on clean-up.

We finish work at around 7:30 with an end-of-day meeting. We relax on the couch and each person gets a chance to say what did and didn’t work for him and to ask the other two for feedback. I might apologize for being distracted during a planning meeting and Asheesh might thank me and Raffi for letting him back. I might apologize for being distracted during a planning meeting and Asheesh might thank me and Raffi for letting him take a phone call while we did the lunch dishes. Since we’re working so closely together in a cramped space, this open communication is essential to staying sane.

As of now, the website has 614 registered users. We’re indexing bugs from 141 projects for our volunteer opportunity finder. In total, there are 954 distinct projects represented on our users’ profiles. They range from small one-person side projects to much larger, international projects such as the Ubuntu project. Right now, the focus within OpenHatch is on getting the word out - our next milestone is having 1024 users.

OpenHatch is more than just work for us. We’re all passionate about Free/Open Source Software and we believe that it's missing an essential human element. We’re working at the nexus of ISTS and the Neukom Institute’s missions, using computing to improve community and collaboration. I’m doing the most fulfilling work of my life, and I sincerely thank ISTS and the Neukom Institute for making this possible with their generous funding.

Phinney continued from page 1

Dartmouth Researchers continued from page 1

Security institutions, headquartered at Dartmouth. The institute coordinates a national cyber security R&D program and helps build bridges between academia, industry and government.

TCIPG team members have been collaborating on work in this area since 2005, with support from the National Science Foundation. They have developed both hardware and software that addresses critical needs in securing the cyber infrastructure of the power grid. Most notably, the researchers developed and implemented a process for protecting message exchanges and a strategy for managing complex security policies in large networks that potentially have thousands of rules about who can access what. TCIPG researchers have also addressed security weaknesses of individual computational devices in substations and homes, which are ripe for financial fraud and cyber-terrorism.

New research aims to integrate information technologies with real-time authentication, integrity, and confidentiality, and hardware and software that resists and tolerates attempts at intrusion without compromising performance. Researchers hope to implement systems that allow for wide-area monitoring and control, respond to and better control demands for energy load, and better provide for the plug-in needs of hybrid electric vehicles.

“We are hoping to implement systems that allow for wide-area monitoring and control, respond to and better control demands for energy load, and better provide for the plug-in needs of hybrid electric vehicles.”

Sinclair to Deliver Seminar on “The Economics of Information Security”

From identity theft to password choice, malicious hackers to social engineering attacks, a host of human factors influence the success or failure of computer security in modern society. This spring, Sara “Scout” Sinclair, PhD candidate in the Department of Computer Science will present a new seminar course on “The Economics of Information Security.”

In this course, students will use economics, psychology, organizational theory, and principles of computer usability to study the problems that arise at the intersection of secure computer systems and human beings. The focus of the course will be on constructing and dissecting arguments about technology and society.

Throughout the seminar Sinclair will draw from research she has both conducted and is conducting through several ISTS-sponsored efforts including the current Information Risk in Data-Oriented Enterprises (IRIDOE) and Trustworthy Information Systems for Healthcare (TISH) projects.

“The Economics of Information Security” is offered as part of Dartmouth’s Institute for Writing & Rhetoric’s First-Year Seminar Program.
Traditional approaches to threat and attack identification have relied on signatures. For example, in the network security domain, intrusion detection systems (IDS) and virus scanners basically look for specific sequences of bytes in packets and files. Similarly, insider threat identification has been largely based on detecting specific known patterns of activity that have been gleaned from previous insider attacks. Such approaches can only detect attacks that are known and are therefore intrinsically unable to identify, detect and respond to so-called “zero-day” exploits.

New approaches to attack identification are needed and many researchers have started to explore techniques that are based on behaviors as opposed to signatures. Applications have emerged in areas as diverse as computer security, insider threat detection, social network analysis, and consumer marketing. Government agencies and industry are increasingly taking interest in research that addresses behavioral properties of networks, people and organizations. In fact, the Defense Advanced Research Projects Agency (DARPA) currently has a call for research proposals that includes cyber anthropology and sociology.

Here at Dartmouth, Dorothy and Walter Gramm Professor of Engineering George Cybenko and his team of graduate students and staff researchers are contributing to this emerging and promising research area. Examples of their work are outlined below.

Web Browsing Behavioral Analysis

As our dependence on the web increases, so does the amount of information that can be gathered about an individual using the Internet. Ecommerce and marketing firms have taken advantage of this fact for years by accumulating information on individuals for purposes ranging from tailoring ad campaigns to personalizing a shopping experience. Although of obvious importance to marketing firms, this data offers potential benefits in other areas as well.

So far, in computer security and intellectual property protection, little attention has been paid to the area of user behavioral profiling. While profiling is generally frowned upon in the context of personal privacy, the ability to accurately profile and depict user activity could eliminate many forms of computer related criminal activity. Using profiling information in the area of computer security can aid significantly in the detection of rogue users, malicious activity, policy violations, and unauthorized data exfiltration, and in many cases will even prevent them from happening.

David Robinson, a Thayer School Ph.D. student, and his advisor, Cybenko, have developed an Online Behavioral Analysis and Modeling Methodology (OBAMM) to accurately and efficiently categorize users based on the semantics of their individual web browsing activities. OBAMM uses URL’s and open source web ontologies to accurately categorize the primary interest areas of an individual and how they are changing. This is achieved by passively “sniffing” network traffic to obtain browsing information, not by instrumentation of the machine’s browser application. Based on what the team terms “reverse category lookup”, OBAMM provides for very accurate categorization models to be built from fairly minimal user data.

Using the methodology, the research team was able to quickly generate profiles summarizing the topics of interest, time spent on each topic, and how many times a topic was visited by a set of experimental users. The profiles provided unique indicators of online behavior and provided insight into a number of key interest areas including malicious compromise and insider threat (demonstrated through activity outside of normal work hours).

Preliminary research in the use of OBAMM has convinced the team that creating models of user behavior is the first step in a process that will help in the early identification of the intent to illegitimately distribute sensitive information. Future research is necessary to determine if behavior profiling is a usable and morally justifiable way of limiting an organizations exposure to other types of intellectual property related risks.

Human Behavioral Modeling Language

Professor Cybenko’s team also is conducting research that invites a broader look at behavioral modeling by developing a modeling language which has applications in a variety of domains. The Human Behavioral Modeling Language (HBML) was created to profile and track dynamic objects in a human terrain. The team believes that a common framework for discussing behaviors of people, networks, and engineered systems is both possible and much needed. Their work has been informed by previous research on process modeling and detection across several application areas.

The research team notes applications of HBML across several domains including:

- **Cyber**: Network use profiling (email use, web site visits, file server downloads)
- **Social**: Interactions (meetings, email, collaborating, calls)
- **Spatial**: Tracking (frequented locations)
- **Logistics**: Travel, purchases, etc.

By taking a holistic view of these domains and considering the three major tasks of human behavioral analysis (anomaly detection, classification, and prediction) HBML can be applied to address complex problems. One such example the research team points to is in the context of an intelligence problem focusing on a terrorist cell. Through anomaly detection, HBML can help to: identify anomalous or “abnormal behaviors” in individuals of interest or groupings of persons of interest, classify individuals as a leader or go-betweens for groupings of cells, and predict individual destinations based on known behavior patterns.

The team expects that the majority of scenarios encountered may be addressed with a simple behavioral modeling methodology. It is their hope that this introductory research provides a starting point in a dialogue leading to the development of a common framework for the systematic analysis of behaviors of people, networks and engineered systems.

Note: Professor George Cybenko recently presented on a related topic at the “Workshop on Policy, Law and Technology for Cyber Security: Bridging the Gap between Policy, Law and Technology” in San Francisco, California.
Smithayer ’12 Awarded Internship Grant for the Spring 2010 Term

ISTS and the Neukom Institute have awarded their internship grant for the Spring 2010 term to Emma Smithayer ’12. Emma will work with two non-profit organizations in Montevideo, Uruguay in association with the One Laptop Per Child program.

In December 2009, the Uruguayan government program, Plan Ceibal, completed its distribution of nearly 400,000 laptops to every public primary school student and teacher. Emma will work with Blogging Desde Infancia (Blogging Since Infancy), which runs blogging workshops for children across the country where volunteers show kids how to use blogs and other social media tools. She will also volunteer with Flor de Ceibo, which is based at the University of the Republic, Uruguay’s largest university. Flor de Ceibo provides general support by assisting in classrooms and organizing events for parents.

We’ll keep up with Emma during the Spring term through periodic updates she’ll post to her blog at http://atermwithplanceibal.wordpress.com. For interested students, the Summer 2010 internship grant applications are due on April 28th. Additional information can be found at http://www.ists.dartmouth.edu/opportunities/internship-program/index.html.

Student’s Participate in Federally Funded Research

Professor Sean Smith, along with Jack Bowman ’11, Amy Zhang ’13, and PhD student Scout Sinclair, is studying how physicians at Dartmouth-Hitchcock Medical Center in Lebanon, N.H., use information technology to handle secure data. One of nearly 100 Dartmouth research projects funded by the American Recovery and Reinvestment Act (ARRA), their study is part of Dartmouth’s Trustworthy Information Systems for Healthcare project (TISH).

“People try hard to do the right thing, with respect to information security, while still getting their jobs done,” says Sinclair. “However, in something like medicine, where the job is saving lives, getting the job done takes priority.” The goal of TISH is to improve security by removing that conflict.

Smith emphasizes the opportunity the project provides to the campus as well. “These undergraduate and graduate students are learning as they contribute to a study which makes a real difference in the world,” he says.

Since President Obama signed the ARRA on February 17, 2009, Dartmouth has received $38.8 million in funding from a variety of federal agencies.

Note: Article originally published in the Winter 2010 issue of Dartmouth Life.

Securing the eCampus

This summer ISTS and Peter Kiewit Computing Services (PKCS) will sponsor their fourth annual Securing the eCampus conference at Dartmouth College. As always, the overarching topic is information security on college campuses. This year’s conference will focus specifically on issues of cloud computing security, e-discovery, current threats, and security and privacy in social networking.

The conference will bring CIOs and CISOs from academic institutions across the country to Hanover, NH. The first day of the conference will offer something new to participants. At a small additional cost, eCampus will offer workshops for information security professionals from educational institutions on such topics as using cloud servers securely and how to best conduct self-auditing.

Day two will feature our traditional offering of presentations from leaders in the information security field. This year, the organizers plan to feature speakers that will address issues of privacy, data leaks, cybercrime, and current threats, as well as a panel discussion on e-discovery and cloud computing. The third day will include break-out sessions that allow participants to discuss specific topic areas in smaller groups and in a more informal setting. Topics will range from e-discovery for higher education to risk assessment programs to security awareness and cyber bullying. Additional details about the venue, agenda, lodging, and more is, or soon will be, available at http://www.ists.dartmouth.edu/events/ecampus.
Postdoc Profile

Timothy Stablein joined ISTS in January 2010 as a Postdoctoral Research Fellow working with Denise Anthony, Associate Professor of Sociology and Research Director of ISTS.

What are you working on at ISTS?
At ISTS, I am working on the Trustworthy Information Systems for Healthcare (TISH) project. This is an interdisciplinary collaboration through which I am researching social informatics of information technology in healthcare organizations. In particular, we are interested in understanding perceptions of the pros and cons of electronic medical records among hospital personnel and patients and subsequent issues surrounding privacy and security. I come to the project as a qualitative researcher and will focus my efforts on collecting, managing, and analyzing interview data.

What are your primary research interests?
I have a variety of research and methodological interests. I earned my Ph.D. degree in Sociology from the University of Connecticut in January 2009. My graduate research employed an ethnographic and interpretive approach to understand the transitional nature of street life among homeless and at-risk youth and young adults. I have also worked in survey research, conducting substance abuse needs assessments and examining patient safety and medical errors. I have had wonderful opportunities to explore many facets of social science research and methods, with my prevailing research interests centering on the sociology of deviance and more recently medical sociology.

How did you decide to become a social scientist?
A lot of people have these great stories about how they knew what they wanted to do from an early age. I wish I could tell you that I wanted to be a social science researcher at the age of four, but it took a bit more time for me to develop these interests. My interests in the social sciences began as a college student and were developed over the course of many years. When I started college, I majored in archeology for a short while. This was my first exposure to the social sciences. I was fascinated by human history and culture, but I also had in interest in understanding contemporary social problems and human organization. During that time I was exposed to a variety of courses in the social sciences and found sociology to be the most pertinent and fascinating. I changed my major to sociology and from there it took a number of years to develop specific research and methodological interests. These were gained by immersing myself in a variety of research settings where I gained an understanding about what I did and did not like about different aspects of the discipline. To this day my interests are still evolving.

What advice would you offer to someone considering going into your field?
Of course I have a bias and would encourage everyone to seek out some aspect of the social sciences, if only to enhance your understanding of the social world around you. It is an ideal and necessary accompaniment to most occupations.

For someone considering a career in sociology I would encourage you to go for it! There are many important areas of research that one can immerse themselves in. A good way to begin is to seek out people who are working on topics and projects that interest you.

I do not think it takes a special kind of person to be a sociologist. One just has to be interested in learning about human organization, interaction, and social structural forces that shape the trajectories of people’s lives. From there you will find it only natural and necessary to learn the methods to systematically observe and interpret those phenomena.

Of what professional accomplishment are you most proud?
As a young sociologist I hope that my proudest and best accomplishments are yet to come. Thus far, I would have to say that my richest experience and proudest accomplishment as a sociologist is related to my research with homeless young people. These youth and young adults felt an overwhelming sense of alienation and often isolated themselves from social service providers. Yet, when I approached them on the street they graciously welcomed me into their lives. Each participant came to me with a unique perspective and together they wove a picture of their personal histories and lives on the street. I am proud of this accomplishment because it epitomized why I got into this work. Though my work thus far has taken me in multiple directions, I am proud to be part of a discipline that continually seeks to evaluate and understand the pressing social problems of our day and the organizational aspects of everyday life.

Dartmouth Computing Services Establishes “Mini Me Network”

The “Mini Me Network” is an isolated environment composed of network equipment donated by Cisco Systems for use in information security research and education. The units are configured identically to those used by the College’s production system. Students participating in the school’s Cyber Security Initiative (CSI) get access to this environment for security testing and assessment purposes under the supervision of Computing Services’ network engineers.

“Interacting with production equipment tends to happen late, or never, in a student’s academic career, which leads to many critical skills having to be learned on the job,” said ISTS affiliate and CSI collaborator Sergey Bratus. “We recognize the importance of introducing students to real production environments early in their studies and work to establish a trust between the students and the system administrators.”

Note: See the November/December 2009 issue of IEEE Security & Privacy for an article on the Cyber Security Initiative by Dartmouth Computing Service’s David Bucciero and Adam Goldstein.
Upcoming Speakers

April 7, 2010
Kevin Fu, Ph.D.
Assistant Professor
Department of Computer Science
University of Massachusetts Amherst

April 15, 2010
Latanya Sweeney, Ph.D.
Distinguished Career Professor
School of Computer Science
Institute for Software Research
Carnegie Mellon University

May 5, 2010
Umesh Shankar, Ph.D.
Google Health

More information on upcoming events can be found at http://www.ists.dartmouth.edu/events.