Dartmouth launches network security study

June 10 2008

Kotz (left) and Bucciero prepare to launch DIST. (photo by Kawakahi Amina '09)

A team of Dartmouth researchers is preparing to launch a project that examines the campus wireless computer traffic in an effort to learn how the network is used and how to best maintain its security. The project is called the Dartmouth Internet Security Testbed, or DIST.

"Our campus environment is the perfect place for this project because we can examine live network activity at scale and in real time," says David Kotz, professor of computer science and the principal investigator on the DIST initiative. "We've worked in laboratory settings with controlled parameters; now it's time for a live, real-world test. For organizations that depend on their wireless networks, like we do, this research should prove invaluable." Kotz is working closely with Dartmouth's Peter Kiewit Computing Services Department.

DIST will develop and evaluate current sensing methods for monitoring the multiple wireless networks at Dartmouth to gather real-time data. Researchers hope to learn how to quickly discover patterns that may indicate malicious activity, and determine the best way to resolve those situations. Kotz explains that the scope and scale of this project is unique within the academic research community, and it will improve network security technology and practices for all Internet users. For example, DIST may help detect unauthorized access points, which can be used to steal users' passwords.

The project is funded by the Department of Homeland Security, through Dartmouth's Institute for Security Technology Studies. In addition to developing and testing technology, DIST will serve as a model for how other enterprises can secure their wireless networks.

The researchers carefully designed their studies to protect the privacy of all campus network users. The aim is to preserve the research quality of the data without compromising user privacy. Numerous procedures are in place to collect data in a way that makes it anonymous, where the user is never identified or associated with his or her network activity. The researchers do not examine any of the content of wireless network traffic; they only see the "headers," the information that distinguishes packets of data from a request to connect to the wireless network.

The headers indicate the size and origin of the data (a laptop or access point), but not the type of data or anything about the contents of the communication. The identity of the individual wireless device is replaced by a random identifier. The researchers also record the specific wireless network being used, whether it's Dartmouth Secure, Dartmouth Public, or Dartmouth Library.

"Privacy is paramount in this research effort," says Kotz. "We've ensured that strict processes are in place to monitor the project to protect

the privacy of our Wi-Fi users."

David Bucciero, Director of Technical Services for the Peter Kiewit Computing Services Department, chairs Dartmouth's Cyber Security Initiative and is very excited about DIST. "I think the findings coming out of DIST will greatly benefit the Cyber Security Initiative. It's kind of like having a computer security safety net protecting us," he says. The Cyber Security Initiative, a campus-wide computing security effort, works to improve the security of the College's information systems through research interests and practical applications. Bucciero's team has been working closely with Kotz to make sure that DIST and his initiative work in concert.

In addition, DIST has been approved by Dartmouth's Committee for the Protection of Human Subjects, by the Kiewit Computing Services Department, and by the administrators or managers of buildings where new equipment will be installed.

Technicians will be installing DIST equipment in a few locations. DIST deployments are planned or underway in Sudikoff, Collis, Baker/Berry, Carson, Burke, Hitchcock residence hall, Cummings and MacLean at the Thayer School of Engineering, and Byrne and Murdough at the Tuck School of Business. Signage will be posted in all locations that alerts Wi-Fi users to the research project.

For more information about DIST, visit the project web site at www.cs.dartmouth.edu/~dist .

Source: Dartmouth College