

The Dartmouth Cyber Security Initiative

Faculty, Staff, and Students Work Together

Three students huddle around a laptop in a dormitory basement late on a Friday night. One walks over to a vending machine and swipes a dining card while the others stare intently at snippets of network traffic displayed on the screen. With a click and

ing staff sought assistance from researchers at the Dartmouth Institute for Security and Technology Studies (ISTS—now the Institute for Security, Technology, and Society). This led to the involvement of a PhD student with significant computer-security and digital-forensics experience. This student greatly assisted staff with the incident response and analysis. Computing Services directors were especially impressed when the findings they received from a well-respected (and expensive) security firm paled in comparison to the student's report.

In the aftermath of this compromise, the Computing Services directors and the ISTS researchers met to discuss the next steps in securing Dartmouth's information systems. Everyone agreed that a full security review of the Dartmouth network and servers was in order but that the cost of hiring an outside firm to perform it would be prohibitive. On the basis of the positive experience with the graduate student, the group suggested that students could assist with this assessment.

Faculty from the Department of Computer Science and the Thayer School of Engineering thought this idea fit within Dartmouth's decades-old "Kemeny tradition." John Kemeny, former Dartmouth president and co-inventor of Basic, advocated putting cutting-edge information technology in front of students. With all involved parties agreeing on

a whirl, the machine drops its product, and the students break into wide grins.

This vending machine was part of a pilot project instituted by Dartmouth College's vending machine supplier. To defray the network cabling cost, the supplier had configured these new machines to use Dartmouth's wireless network. With some protocol analysis, hijacked connections, and crafted packets, the students successfully tricked the machine into releasing items without charging a dining account. So what do the students do after figuring out this modern equivalent of a dollar on a string? They don't empty the machine and sell the items at a discount to their partying dorm-mates. Instead, they go back to their room and write a detailed report of their findings, which they send to their research advisors and the Dartmouth IT security staff.

These students are participants in the Dartmouth College Cyber Security Initiative (CSI; www.dartmouth.edu/comp/security/csi), a collaboration between faculty, staff, and students that focuses on projects to improve the security

of Dartmouth's information systems. A director from Dartmouth Computing Services asked the students to assess the vending machines' security. The vendor was notified of the study results but was unwilling to secure the wireless communication. So, Dartmouth insisted that all new vending machines be wired to the network.

The vending machine hack is an example of the type of work the CSI Team performs and illustrates why the program is a success. Dartmouth benefits from results that enable it to make its information systems more secure. The students obtain experience in real-world, hands-on problem solving with their institution's full support. Others see that student enthusiasm for security analysis and penetration studies is an untapped resource and that the students can be trusted to perform such tasks.

Looking Back

The seeds for the Dartmouth CSI were planted in the summer of 2004. Several Dartmouth College administrative servers were compromised, and the comput-

ADAM
GOLDSTEIN
AND DAVID
BUCCIERO
*Dartmouth
College*

the proposed initiative's potential, a group comprising Computing Services staff, ISTS researchers, and faculty set to work to make it a reality. This group became the CSI management team.

Essentially, the CSI management team proposed that students undertake red-team studies of Dartmouth information systems. To allow this, they had to ensure that proper safeguards against student misconduct were in place. The CSI management team worked with the Dartmouth General Counsel's Office to establish the ground rules. The General Counsel determined that students had to agree to a background check, sign a confidentiality statement, and reassert that they would abide by the Dartmouth Student Code of Conduct. In addition, staff, faculty, and researchers would provide careful oversight of the student work, and staff would closely supervise any testing of highly critical or sensitive systems. By spring 2006, the CSI faculty members assembled a group of six interested students, and the initiative was under way.

Following the adage "if you teach a man to fish, you feed him for life," the CSI management team brought in an outside security consultant to instruct the staff and students on security assessment techniques. The consultant performed a thorough review of a critical subnet, training the student team in the process. Over the next few months, the students automated many steps of that process and assessed more than 10,000 hosts on 230 subnets. The procedures and tools they developed were so effective that Computing Services staff uses them to perform monthly assessments.

A Case Study in Collaboration

After this initial project's success, the Computing Services administration was convinced of the

program's value and committed to ongoing support of the initiative. They purchased equipment, contributed a portion of graduate student stipends, and paid undergraduates for up to 10 hours of work a week. Work on the student team typically follows Dartmouth's four-term calendar. Students sign up on a term-by-term basis, with most students participating for multiple terms. A typical team includes one or two graduate students serving as mentors for the undergraduates. Over the past year, students participating included two PhD students, three master's students, and six undergraduates.

Past Projects

The CSI team has been involved in a number of projects over the past three years. Here, we look at three examples.

Wireless security. The CSI team worked with Computing Services to research, test, design, implement, and deploy Dartmouth's secure wireless network. By demonstrating a variety of wireless attacks, including man-in-the-middle and session hijacking with rogue devices, the CSI team illustrated several weaknesses in popular wireless security methods such as PEAP (Protected Extensible Authentication Protocol) and EAP-TTLS (Extensible Authentication Protocol-Tunneled Transport Layer Security). On the basis of these findings, Dartmouth implemented a wireless security

Encryption and authentication testing.

Working with researchers from the Dartmouth PKI Lab, the CSI team tested Dartmouth's authentication systems. In doing so, they uncovered a cryptographic weakness in one of Dartmouth's most commonly used authentication processes. Using a single PC, the team developed a procedure that let them crack anyone's password within nine hours. As a result, Dartmouth changed its cryptosystem.

Security review of proposed technologies.

While performing security tests of new technologies that Dartmouth was considering deploying, the CSI team discovered vulnerabilities in several systems. In addition to the wireless vending machines, the team discovered security holes in IP-to-TV converters and an enterprise printing application. The team reported these vulnerabilities to the vendors, who used the findings to improve their products' security.

Further Benefits and Growth

In addition to hands-on experience, the students involved in the CSI have benefited academically. Several of them have been able to share their experiences in doing these projects and other CSI work at conferences around the country. These conferences have ranged from EDUCAUSE and other events associated with higher education to well-known practitioner

Dartmouth benefits from results that enable it to make its information systems more secure. The students obtain experience in real-world, hands-on problem solving with their institution's full support.

architecture that uses public key infrastructure (PKI) technology to support encryption and supports two-factor authentication.

conferences such as Blackhat and ToorCon. Students have also incorporated their CSI work into course projects, journal papers,

and, in one case, an open-source software project that won a competitive Dartmouth award.

Over the past year, other organizations have taken notice of Dartmouth CSI and offered support. Cisco's Information Assurance Group (CIAG) donated a wide range of enterprise-grade equipment to the CSI for building a network security lab. The program also recently received a capacity-building grant from the US Department of Defense's Information Assurance Scholarship Program (IASP). These funds will help provide additional equipment and enable more students to participate.

Current Projects

With the program now entering its fourth academic year, CSI teams are working on a number of interesting projects. Here are three.

Public computing and privacy.

A team is gathering data from the College's public computers on how frequently students leave files on the system (for example, files copied to the desktop, or folders or files with personal or sensitive data in temporary folders that aren't deleted at the end of a session), leave browsers open and connected to Web sites, or close the browser but leave session cookies behind (because they didn't log off the Web site).

Cloud-computing security. Another group of students has been working on identifying the benefits and risks of popular cloud server providers.

Network security lab. With the donated Cisco equipment, a CSI team will test and analyze known and emerging layer 2 and layer 3 attack techniques.

Lessons Learned

Although the program results have met expectations, the CSI organizers have uncovered a few po-

tential problems. Student schedules can make project planning difficult. What with exam schedules, class projects, and extracurricular activities, trying to establish project timelines is a challenge. The management team has found that assigning a student or a group of students one task at a time is the most effective approach. To keep things moving, the student team and CSI management team meet separately once a week to assign tasks, report on problems, discuss issues, and collaborate on the more complex problems.

The CSI management team will address the challenge of involving students from disciplines other than computer science and engineering. They hope that a proposed project regarding security metrics will attract business students and those interested in statistical analysis. Similarly, they're attempting to recruit communications and visual-arts students to help increase user awareness.

Perhaps the most significant sign of success for the CSI is that Dartmouth's administration, participating faculty, and student team members are all pleased with the results. This isn't surprising. The collaborative approach benefits Dartmouth by tapping into the Dartmouth community's IT security expertise, while embracing the academic mission by providing learning experiences for students.

We hope that the Dartmouth CSI will serve as a model for other institutions, not only as an example of successful collaboration between administrators and academics but also as confirmation that students can be trusted to assist computer security efforts and that their skill and enthusiasm are valuable resources. Ultimately, information system security is a campus-wide concern, and the entire campus community can play

a role in protecting the school's information systems. And, as evidenced by a group of students unlocking the mysteries of a wireless vending machine, that role can be fun as well. □

Acknowledgments

The CSI staff are David Bucciero, Adam Goldstein, Frank Archambeault, Steven Nyman, Scott Rea, William Stearns, and Ellen Young. The CSI faculty are Vincent Berk, Sergey Bratus, George Cybenko, David Kotz, Anna Shubina, and Sean Smith.

Adam Goldstein is the IT security engineer with Peter Kiewit Computing Services at Dartmouth College. Contact him at adam.goldstein@dartmouth.edu.

David Bucciero is the director of technical services for Peter Kiewit Computing Services at Dartmouth College and chairs Dartmouth's Cyber Security Initiative. Contact him at david.l.bucciero@dartmouth.edu.