COURSE LEADS STUDENTS THROUGH

The Dark World of Computer Security

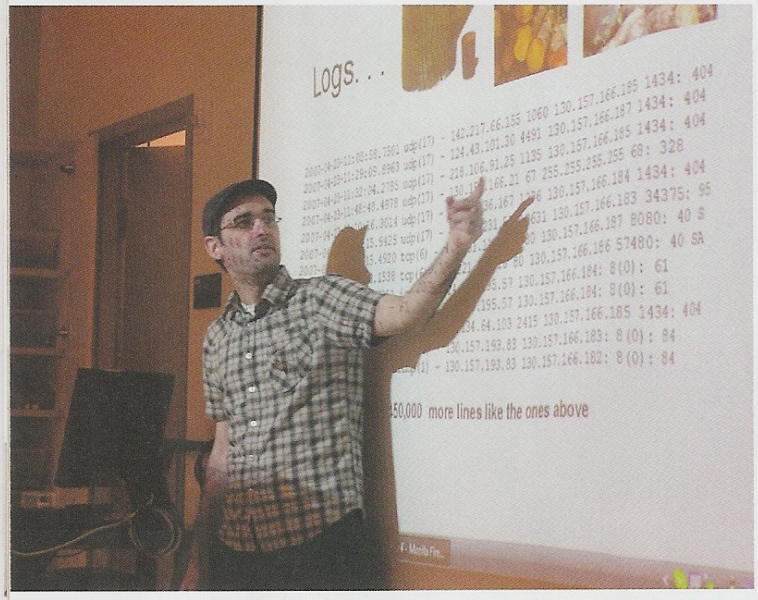
by Jean Wasp

From fork bombs to worms to viruses called Cookie Monster, computer-science students at Sonoma State University are exploring the world of "malicious software" as part of the computer security curriculum. By cautiously confining a single computer network on campus to a small mobile cart with four computers running on different operating systems, Professor George Ledin is teaching students about the dark world of computer viruses.

In a course about "malware," students are learning the intricacies of how computer viruses are constructed in much the same way biology students learn about the intricacies of bacterial organisms and other life forms that cause disease.

Professor George Ledin (center) with John Sullins (left), philosophy professor who teaches the ethics portion of the malware course. Roger Mamer (right), systems specialist, supports the technical work of the professors and students. Photo by Charlie Gesell.


/ now send anonymous email messages containing this php source co
/ in the hopes that more and more people will run this script.
/ get a list of
dresses to spam, then put each email into
xec("wget htt
onoma.edu/~btietz/cs340/emailList emailL
// Open file
SemailList =
// Read in t
SemailListStr
// Now
fclo
Se
$from
$url =
$mess
#mail



Student Mike Drew demonstrates the workings of a "Honeypot," a system on the Internet that is expressly set up to attract and "trap" people who attempt to penetrate other people's computers.

Ledin hopes to create a new career path for computer science students who can join the ranks of computer security professionals to protect from the perils of cyber attacks.

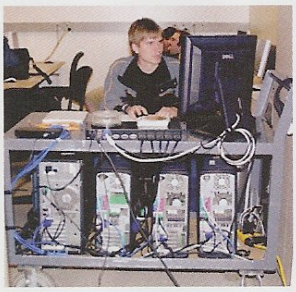
In the brightly lit CS lab in Darwin 25, one of Ledin's students, Dan Fogle, shows how a not-so-cuddly Cookie Monster works, persisting in its demands for a cookie (an imaginary digital biscuit) and, if denied the treat, activating hidden commands that cause the machine to be crippled. Thomas Fynan demonstrates the power of his "forum flooder," where phony commentary manifests in a forum or blog giving an indication there is a groundswell of opinion on a particular issue where none really exists.

Although the concepts are not new, students such as Fogle and Fynan have been able to write the malware themselves and lead the class to a better understanding of how some viruses can alter or destroy the machine's operating system registry or do other damage while the user is unaware there is anything unusual going on.

The viruses written by the students work undetected by all antivirus software. Some crash not only all previous operating systems, such as Windows 98, Windows 2000, and Windows XP, but also the newest one, Vista. Others lay hidden as an "unwanted tenant" logging the keystrokes of the unwary user.

That same day another student, Lincoln Peters, demonstrates the workings of his "fork bomb," an utterly simple but extremely annoying and potentially deadly code segment that fills up the computer screen with a never-ending proliferation of windows.

The goal is for students to use their knowledge of the "dark side" of programming to build future computer systems that are better equipped to guard against and even combat these malicious programs. Other



Student Lincoln Peters sits at the helm of a closed network of four operating systems which are used to test malware he has designed. Photo by Roger Mamer.

student projects have been produced by Brian Tietz, Grant Joy, Chris Mefford, Ben Corr, Travis Kool and Mike Drew.

"Learning about viruses and malware is like learning a martial art. One has to learn how to attack in order to develop an effective defense", says John Sullins, a philosophy professor who is working with Ledin on the ethics of the course.

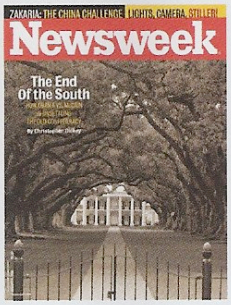
"Ledin's class provides students with an uncommon opportunity to learn not only how to react and defend against malicious computer programs, but also how they are used and the logic behind their construction."

"Ledin is like a sensei in a virtual dojo; he not only instructs his students in the nuts and bolts of the creation of malicious software, but he also guides their understanding of when one should, and shouldn't, use the skills they are learning in his class." Sullins says this gives the students an increased ability to protect themselves, their friends, family and employers from the harm that malicious software can do.

The malware course is based on the ethical arguments presented by Ledin in his widely-disseminated editorial published in the January 2005 issue of the Communications of the Association for Computing Machinery, the worldwide society of computer scientists and computing specialists.

It is essential, Ledin argues, that computer scientists know malware as intimately as life scientists know biological viruses, bacteria, parasites, and other disease-causing microorganisms.

"We cannot afford to wait for the computer equivalent of 9/11 to learn what the bad guys were doing. Not teaching viruses and worms is a prescription for disaster," he says.



See the story and video featured in the Aug. 11, 2008 issue of *Newsweek* entitled "The Bug Man is a Pest" at http://www.newsweek.com/id/150465.