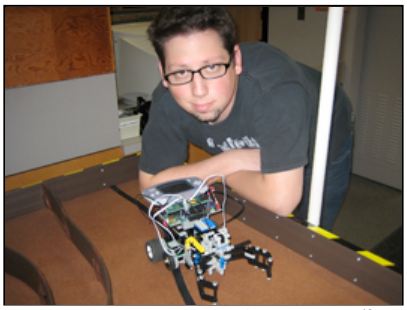
- home
- music & nightlife
- movies
- the arts
- restaurants
- classifieds
- columns
- news & features
  - SONOMA / NAPA / MARIN
  - SILICON VALLEY
  - SANTA CRUZ COUNTY
- the papers
- advertise
- about us
- contact

Virtual Virtues

Will we be ready when bad things happen to good computers?

By Bruce Robinson



Courtesy Marc Helfman

This is Your Brain on Legos: SRJC student Kevin Keita shows his mini-bot constructed for Marc Helfman's design class

The basement room could hardly be more plain: unadorned windowless white concrete walls with fluorescent light fixtures hanging beneath industrial piping that snakes across the ceiling. Within this softly humming bunker, a thin, bearded young man is demonstrating his new "fork bomb," a few lines of code that can force a computer defended with popular antivirus software to fill its hard-drive with useless cloned repetitions, crippling the machine within minutes and potentially rendering it useless. Observing from one side, George Ledin nods approvingly.

A professor of computer science at Sonoma State University, Ledin is watching the final presentations by six students from his quietly controversial "malware" course, an upper division class that studies an array of digital demons—viruses, worms, Trojan horses and more—and then asks the participants to devise one of their own. Their demonstrations, each representing a different sort of surreptitious approach and conducted in a meticulously isolated or "sterile" digital environment, are swiftly and methodically successful.

Offered for the first time last spring (a second section is underway now), Ledin's class is, to his dismay, the only one of its kind offered at any university in the country, and it was reluctantly added to the curriculum only after months of urging by the professor.

The cadre of carefully chosen students have "seen the code of viruses and worms, something that computer professionals typically have never seen," Ledin explains softly but seriously. "This is equivalent to a physician or nurse or any health practitioner never actually seeing anything microscopic.

"The idea that only the bad guys know how to do it is, to me, a travesty," he continues. "If my students, who are beginners, can slip by all of the antiviral companies, then you can imagine what the Chinese and others are doing.

"Why is it that we aren't more proactive? It's absurd not to have any preparation."

Ledin's advocacy has made him a pariah in the realm of antivirus software makers. The major American companies not only refused to share information or participate in the SSU class, the professor says, but also vowed not to hire any graduating students who have taken it.

There is little love lost on Ledin's side of that exchange, ether. He sees antivirus software, collectively, as "a complete placebo," incapable of providing any meaningful protection from new assaults.

"There isn't a single instance of a virus company thwarting a virus before it attacks," Ledin scowls. "This is a $4 billion industry based on no science."

The creations of the students in Marc Helfman's SRJC class are less ominous and more tangible than the malware concocted in Ledin's lab. Assembled from a huge tray of Lego pieces, according to an outline prepared by the instructor, these small, crablike rolling robots use repurposed Gameboys as their "brains." But the bots themselves are a means to an end, the tools used by Helfman's students to develop and apply their programming skills.

Offered for the first time last fall (and again this semester), Robotics Design and Programming is essentially a lab for students working with C, a widely used computer programming language. The students' assignment is to craft instructions that will direct the robots to perform a series of moderately complex tasks: following a curving wall at a uniform distance, locating and removing an object from a designated area, distinguishing between light and dark colored targets and treating them differently.

"The students write a program on their computer in C and then, by hooking a cable into the contraption, they can download the program and connect the motors and various sensors, and then the robot's able to do whatever they've told it to do," Helfman explains. But once the instructions are downloaded, these robots are strictly hands-off.

"The intelligence is all in the program," Helfman continues. "Once I press the button, it's on its own. In this class—and most competitions—if you touch the robot, that's it, you're out of the game."

The "game" in this class is a complex final exam, played out on a tabletop course set up to simulate a rescue or hazardous material removal situation. The students' bots compete to quickly find their way into the correct chamber, search for and recognize the target object, then grasp it and remove it to the specified safe location.

"It's a cumulative experience where they get to put together everything they've learned," Helfman says, "and they were by and large successful with it."

Gameboy-driven Lego-bots and home-made computer viruses may not seem to have much in common beyond their tech-based origins, but John Sullins sees a connecting thread. This semester, Sullins, a philosophy professor at SSU, is introducing a new course he's titled "Digital Being" to begin exploring, among other things, the ethical implications of robotics.

"Are robots the types of things that deserve our moral consideration? How do they change our relationships with one another?" he asks. "Are some of my moral rights extended to my machines that are doing my bidding? What are the rights that we should extend to our technologies as they become more and more sentient? These are all very deep and difficult issues, things that have only really been thought about in science fiction."

Sullins has also been carefully—and supportively—observing Ledin's malware course experiment, keenly focused on the ethical question, "Should you teach someone how to use this very dangerous piece of technology?"

His answer echoes Ledin's reasoning. "We should teach it because it allows us to deal with the reality that our students are going to face. They're going to have to deal with this technology and understand it in order to defeat it or to use it beneficently."

But Sullins' considerations go further, to question if even the term "malware" is unfairly pejorative. "The name 'malware' would suggest to you that it's just evil, that everything about it is wrong. But I'm not so sure about that," he reflects. "Is malware really ethically wrong when it's used as a way to maybe combat a tyrannical government?

"Malware has been used in China as a way of breaking down firewalls that prevent [citizens] from seeing the wider Internet, and it's hard for me to say that's necessarily wrong," he continues. "So shouldn't good people know how to use malware as a tool for forcing social change, as a way of disrupting a vicious system?"

John Aycock, a professor at the University of Calgary, is the only other educator in North America who is publicly teaching students how to recognize, write and repel malware. He sees these classes as critical to combating the growing number of cyber threats in the world, such as the mysterious attack that crashed many of the key systems in the Eastern European nation of Estonia early last year.

"The thing we've been worrying about," Aycock says, "is the scale of some of these attacks. If you consider a bunch of bad guys who have 100,000 computers at their disposal which they've stolen access to, what are they going to do with them? Who knows?"

Ledin, who has also been warily pondering such questions, believes that an effective response ultimately lies in developing a comprehensive theoretical framework to understand destructive software, something he worries will take "a decade or two" if and when the effort seriously gets underway.

And even that might not be enough. Faced with the catastrophic consequences of a possible global cyber-terrorist onslaught, Ledin says, "Maybe we need to redesign the computer completely to be immune to this.".

Send a letter to the editor about this story.