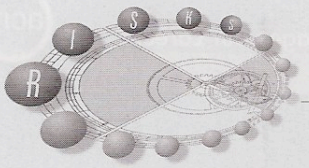

Not Teaching Viruses and Worms Is Harmful

Computer security courses are typically of two kinds. Most are of the first kind: guided tours to concepts and terminology, descriptive courses that inform and acquaint. These courses have few or no prerequisites and little technical content. The second kind of computer security courses is taken primarily by computer science majors. Usually elective courses, they offer a technical menu, often focused on cryptography. Systems, access control models, protocols, policies, and other topics tend to get less coverage.

A critically important topic, viruses and worms, gets the least coverage. Anecdotal and historical information about them may be presented, but source code discussions are rare and programming a virus or worm and their antidotes is seldom required. Not too long ago, crypto was a taboo topic subject to government controls. Developments, such as PGP, helped remove these prohibitions, and serious academic research is now routine. Virus and worm programming should likewise be mainstreamed as a research activity open to students. As previously with crypto, there are barriers to overcome.

The first barrier is the perception of danger. Bioscience and chemistry students conduct experiments with microorganisms and hazardous substances under supervised laboratory conditions. Computer science students should be able to test viruses and worms in safe environments.

The sciences do not shy away from potentially dangerous knowledge. The spread of the West Nile virus across the U.S. has been tracked not just by health officials but researched by students at hundreds of universities. If powerfully lethal viruses such as Ebola cannot be studied, how would vaccines or cures be developed?

Those opposed to teaching these "dangerous" topics compare malicious software to explosives and weapons that are designed to kill, maim, and cause physical destruction. A course that teaches how to write malware may be analogized to a chemistry course that teaches how to make Molotov cocktails or a physics course that teaches how to build nuclear warheads. These are clearly sobering concerns.

There is no doubt that viruses and worms are being investigated for their potential as weapons. The art of cyber war is being taught, secretly, at military academies and espionage agencies. Biological and chemical warfare are also taught. Armed forces, diplomatic management, and intelligence services must be prepared. The dangers of bioterrorism are real and serious; "weaponized" anthrax, for example, is a grave threat.

Using extreme examples of biological warfare agents and nuclear bombs gives the impression that malware is very rare and exotic, when it actually is a relatively common, costly nuisance. It is more useful to compare malware to the many infectious agents that are present in daily life, household diseases such as influenza, malaria, measles, whooping cough, and cholera, which have a huge worldwide impact and are being studied in many laboratories. Research on these diseases is the foundation for our understanding of all infectious agents, from mild to deadly.

The second barrier is moral clarity. Launching malware has serious legal consequences. Is teaching aiding and abetting? Virus and worm study must include a strong ethical component and a review of cases and legislation. Ethical and legal worries are obvious hurdles. Fearing they would be held responsible for anything done by their students, and being already more than adequately overwhelmed by trying to stay with a subject that keeps accelerating, computer science faculties find little incentive to do something that they later might regret.

Computer science students should learn to recognize, analyze, disable, and remove malware. To do so, they must study currently circulating viruses and worms, and program their own. Programming is to computer science what field training is to police work and clinical experience is to surgery. Reading a book is not enough. Why does industry hire convicted hackers as security consultants? Because we have failed to educate our majors.

Which brings us to the third barrier: university faculties' lack of expertise. Most professors have never studied a worm or virus, much less programmed one themselves. Yet, having overcome the first two barriers, most professors will welcome the opportunity to teach the next generation of students to be malware literate. This would help not only with viruses and worms but also with other pests, such as adware, nagware, and spyware. And our graduates would contribute to the public good. C

PAUL WATSON

GEORGE LEDIN, JR. (ledin@sonoma.edu) is the chair of the computer science department at Sonoma State University.