Computers need legal, technical protection

By Joan Herman
Of the Emerald

Art often imitates life. And sometimes life imitates art. Take the movie "War Games," which was about a teenager who broke into the Defense Department's computer systems via his own home computer.

The movie was fictional. The felony charges against a UCLA student, Ronald Austin, who allegedly committed a similar act about two weeks ago, are real.

The physics student, who was ordered to stay away from computers, pleaded innocent to 14 felony charges of deliberately breaking into the Defense Department's computer system. If convicted, he could face a maximum six-year prison term.

Breaking into computer systems, or "hacking," is not new. But it has gained notoriety in the last few years because more hackers are being caught.

Still, no federal laws directly address hackers and the ethics of hacking. Because computers are a relatively new member of society, few people — public and computer experts alike — consider the ethical implications of computer piracy, says Eugene Luks, head of the University's Computer and Information Science department.

"One has to have some sort of ethics and we don't ignore that fact" when teaching computer science classes, Luks says. "There is a social ethic students have to be aware of. A lot of issues are very obvious, but they have to be stated up front."

Breaking into someone else's computer system is no different than peeping through neighbors' curtains or listening in on their private conversations. In essence, hacking infringes upon someone else's rights, he says.

"Would you go to your neighbor's mailbox when they're out of town and read their mail? You woudn't. You have standards."

Dennis Kucera, a computer science and math student, agrees.

As a member of the University's Computing Association Club, Kucera and his friends have discussed computer piracy. Most of his friends "frown upon doing things like that because they've been brought up not to do those things," he says.

"Usually peer pressure is enough to prevent it (hacking)," Kucera says. "Usually they (computer science students) take pride in what they do and they don't tamper around. Most of my friends have an ethic against doing something like that.

"With the time that it takes to do all that, you can be doing more constructive things. You can be doing something intelligent."

According to an Associated Press story, Austin allegedly worked as many as 10 hours a night, for many nights, to break the Defense Department's computer codes.

"I don't know how he got into it," Kucera says. "It would be extremely hard."

But Luks was not surprised by what happened. "He (Austin) was the only one to get caught but what he did, many other people could and probably have done. I certainly have heard of many such stories myself."

Some University students are "certainly clever enough" to do what the UCLA student allegedly did, Luks says. "It's entirely possible that people learn things here that could facilitate crime. We teach a good deal about the inner workings of the computer, and when you learn how to read computer jargon, you can learn (even more) by hacking it out alone."

Usually hackers do just that — hack it out alone, Kucera says. Hackers tend to be loners who "want someone to notice them," he says.

An Aug. 28 article in the New York Times supports Kucera's hypothesis. The article, which transcribes a dialogue between two former hackers, states that electronic pirates consider themselves an elite group as far as ability goes.

But when it comes to society, these modern day pirates are usually outcasts, the article states. They yearn for attention, and possibly through their hacking they hope to gain such notice, surprisingly, — by being caught in the act.

Hackers are generally inquisitve types, the article says. They like to figure things out, such as what a computer's password is, even if it takes them weeks or months.

"It's a game for a lot of computer science students to try and beat the system, says John Benefiel, who programs, installs and repairs computers in the Eugene area.

You don't need to be a genius to crack a computer code, Benefiel says. All it takes is a "little common sense and a little time and you can figure it out."

Most major company's computer systems are tied into the phone lines, just as smaller systems are, he says. By using a modem (a telephone line hookup which is connected to the home computer), you could dial the specific number of a company's computer and connect your personal computer system with a major system, such as the Defense Department's.

Before you can actually get into the other system, though, you must know the system's password, which is where the hacking game becomes somewhat like finding a needle in a haystack.

Undoubtedly the hacking game will become even more difficult, if not nearly impossible to crack, Luks says. "There's going to be a lot of work that goes into making computers more secure. No system is perfect, but there are ways to protect your system." At the University, researchers are examining ways to protect computer systems, Luks says.

Another possible security measure would be putting a warning into the computer system, stating that breaking into computers is illegal and punishable by law.

The Times article suggested programming computers to detect "repeated attacks," or attempts to break into a system. If the computer had a "watchdog" system that could detect such attacks, a hacker would receive a warning message stating such actions are illegal, and every attempt is being made to trace the call.

In the near future, computers may be equipped with voice scans. A person would have to speak into the computer before making any commands, and the scan could detect if the person was authorized to use that system.

At any rate, Luks says, the computer industry will no longer "underestimate the public."

The next move of the hacking "game" is up to corporation's computer programmers, who now must learn to beat the hackers at their own game.

Bloom County Courtesy of Berke Breathed