Using computers in carrying out crime is nothing new. Computers are routinely seized and examined in investigations of gambling, prostitution, illegal drug distribution, pornography, sale of stolen goods, all kinds of theft, money laundering and loan-shark operations.

A specialized subset of computer-aided crime is simulation, in which complex systems are emulated using a computer. For example, simulation was used by a former Marine who was convicted in May 1991 of plotting to murder his wife. Apparently he stored details of 26 steps in a “recipe” file called “murder.” The steps included everything from “How do I kill her?” through “Alibi” and “What to do with the body.”

Simulation was used in a bank fraud in England in the 1970s. A gang of thieves used the system for a complex check kiting operation. Check kiting consists of writing checks alternately from one bank to another faster than the float period during which the deposit exists in the receiving bank but before it has been deducted from the issuing bank. The apparent amount rises like a kite as money shuttles back and forth. Then one day the criminal clears all the money out of the accounts and disappears. Naturally, banks know all about this trick, so any repeated sequence of deposits and withdrawals from one account to another results in a freeze on the accounts until the money actually clears. Knowing this restriction, the criminals in England used 12 banks to shuttle money around. They kept track of exactly which bank was supposed to receive which fraudulent check for what amount drawn on which other bank. The scheme would have worked if the computer hadn't broken down. At that point, the scheme unraveled, with the fraudulent checks bouncing in sequence when account after account was found to be without sufficient funds for the payments. Scotland Yard were alerted to an unusual rash of bad checks all over London. The police traced the conspirators to a room where a computer programmer was desperately trying to fix his broken computer system. Luckily for the banks, the criminals had no backup hardware.

In a corporate environment, if employees know that you will carry out periodic audits of files on your enterprise computer systems, you may dissuade criminal employees from using your property in carrying out their crimes. On the other hand, such audits may lead dishonest people into encrypting incriminating files; a strict policy prohibiting unauthorized use of encryption may help fight that kind of abuse. However, unannounced audits on employees who have not been adequately trained and prepared to meet corporate requirements may cause morale problems, so it's important to discuss the issue with your staff before imposing such routines.

A politically sensitive question about simulation is whether the simulation of crimes by videogame programs contributes to juvenile delinquency. For example, a few years ago, a game was put on the market that gave players points for various forms of arson, including extra points for killing larger numbers of innocent victims. The fire chiefs of the United States protested and the game was withdrawn. There are several sites on the Web that turn criminal hacking into games and glorify criminal hackers; perhaps I’ll look into the status of research on this question for a
NEW! 18-month online Master of Science in Information Assurance offered by Norwich University; see <http://www3.norwich.edu/msia> for full details.


M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at <mkabay@norwich.edu>; Web site at <http://www.mekabay.com/index.htm>.

Copyright © 2002 M. E. Kabay. All rights reserved.

Permission is hereby granted to Network World to distribute this article at will, to post it without limit on any Web site, and to republish it in any way they see fit.