In the last column, I introduced an interesting paper by Richard T. Ainsworth, a lecturer at the Boston University School of Law, who has written about zappers – programs which divert funds for systematic embezzlement of tax obligations. Today I conclude with some of his major findings and comments of my own.

Mr Ainsworth makes an important point about zappers: “Neither certification of ECRs[electronic cash registers], nor technologically-sophisticated audits are effective against Zappers, because Zappers destroy the records they alter. If Zappers are the problem, then a solution will require securing not only the till, but the data within it. Doing this will involve taking some non-traditional steps. It will require that the government become directly involved in the certification of the production and retention process used to produce the primary business records at the point of sale.”

Going beyond the specific subject of zappers, this observation is fundamental to our approach to any software that is deliberately installed to falsify both the accuracy of calculations and the audit trail which would normally be used to catch malfeasance. The only sensible approach to identifying such systems is to run a known set of transactions through the normal processes and then to compare the results against what should have been produced. And such tests must be conducted without warning to the operators of the suspect systems. Remember the strategy we use in seizing static forensic evidence: we make image copies of all the storage media to prevent tampering with the data on the suspect system. In cases of suspected embezzlement via software, I think we have to seize the working system, not only make bitwise copies of the data but also create a clone of the entire system using hardware that’s as close to the original as possible, and then exercise the clone under tight observation using known inputs as if we were conducting a thoroughgoing software quality assurance inspection.

To conclude today’s column, I remind readers of a case from 1998 that illustrates Mr Ainsworth’s point and my elaboration: “In Los Angeles, the district attorneys charged four men with fraud for allegedly installing computer chips in gasoline pumps that cheated consumers by overstating the amounts pumped. The problem came to light when an increasing number of consumers charged that they had been sold more gasoline than the capacity of their gas tanks. However, the fraud was difficult to prove initially because the perpetrators programmed the chips to deliver exactly the right amount of gasoline when asked for five- and ten-gallon amounts — precisely the amounts typically used by inspectors.”

Mr Ainsworth is soliciting comments on his valuable report and I hope that readers will oblige him by sending him suggestions and additional case material to add to his continuing research project.
M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance <http://www.graduate.norwich.edu/infoassurance/> and CTO of the School of Graduate Studies at Norwich University in Northfield, VT. Mich can be reached by e-mail at <mailto:mekabay@gmail.com>; Web site at <http://www.mekabay.com/index.htm>.

Copyright © 2008 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.