This is the second of a pair of articles looking at salami frauds, where tiny thefts are repeated many times.

Peter G. Neumann, in RISKS 18.75, wrote that in January 1997, "Willis Robinson, 22, of Libertytown, Maryland, was sentenced to 10 years in prison (6 of which were suspended) for having reprogrammed his Taco Bell drive-up-window cash register -- causing it to ring up each $2.99 item internally as a 1-cent item, so that he could pocket $2.98 each time. He amassed $3600 before he was caught." Another RISKS correspondent added that management assumed the error was hardware or software and caught the perpetrator only because the idiot bragged about his crime to co-workers.

In Los Angeles in October 1998, 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.

Unfortunately, salami attacks are designed to be difficult to detect. The only hope is that random audits, especially of financial data, will pick up a pattern of discrepancies and lead to discovery. As any accountant will warn, even a tiny error must be tracked down, since it may indicate a much larger problem. For example, Cliff Stoll's famous adventures tracking down spies in the Internet began with an unexplained $0.75 discrepancy between two different resource accounting systems on UNIX computers at the Keck Observatory of the Lawrence Berkeley Laboratories. Stoll's determination to understand how the problem could have occurred revealed an unknown user; investigation led to the discovery that resource-accounting records were being modified to remove evidence of system use. The rest of the story is told in Stoll’s book, _The Cuckoo’s Egg_ (1989, Pocket Books: Simon & Schuster, New York – ISBN 0-671-72688-9).

If more of us paid attention to anomalies, we'd be in better shape to fight the salami rogues. Computer systems are deterministic machines – at least where application programs are concerned. Any error has a cause. Looking for the causes of discrepancies will seriously hamper the perpetrators of salami attacks. From a systems development standpoint, such scams reinforce the critical importance of sound quality assurance throughout the software development life cycle.

Moral: don’t ignore what appear to be errors in computer-based financial or other accounting systems. And next time you audit your accounting system, don’t overlook $3.8 billion dollars of unexplained profit, either.

***

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@compuserve.com>. He invites inquiries about his information security and operations management courses and consulting services. Visit his Web site at <http://www.mekabay.com/index.htm> for papers and course materials on information technology, security and management.

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.