

Salami Fraud

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

One type of computer crime that gets mentioned in introductory courses or in conversations among security experts is the salami fraud. In the salami technique, criminals steal money or resources a bit at a time. Two different etymologies are circulating about the origins of this term. One school of security specialists claim that it refers to slicing the data thin – like a salami. Others argue that it means building up a significant object or amount from tiny scraps – like a salami.

The classic story about a salami attack is the old “collect-the-roundoff” trick. In this scam, a programmer modifies the arithmetic routines such as interest computations. Typically, the calculations are carried out to several decimal places beyond the customary 2 or 3 kept for financial records. For example, when currency is in dollars, the roundoff goes up to the nearest penny about half the time and down the rest of the time. If the programmer arranges to collect these fractions of pennies in a separate account, a sizable fund can grow with no warning to the financial institution.

More daring salamis slice off larger amounts. The security literature includes case studies in which an embezzler removed \$0.20 to \$0.30 from hundreds of accounts two or three times a year. These thefts were not discovered or reported: most victims wouldn't bother finding the reasons for such small discrepancies. Other salamis have used bank service charges – increasing the cost of a check by \$0.05, for example.

In another scam, two programmers made their payroll program increase the federal withholding amounts by a few cents per pay period for hundreds of fellow employees. The excess payments were credited to the programmers' withholding accounts instead of to the victims' accounts. At income-tax time the following year, the thieves received fat refunds from Internal Revenue.

In January 1993, four executives of a rental-car franchise in Florida were charged with defrauding at least 47,000 customers using a salami technique. The federal grand jury in Fort Lauderdale claimed that the defendants modified a computer billing program to add five extra gallons to the actual gas tank capacity of their vehicles. From 1988 through 1991, every customer who returned a car without topping it off ended up paying inflated rates for an inflated total of gasoline. The thefts ranged from \$2 to \$15 per customer – rather thick slices of salami but nonetheless difficult for the victims to detect.

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 correspondent adds that management assumed the error was hardware or software and only caught the perpetrator when he bragged about his crime to co-workers." (Peter G. Neumann writing in RISK 18.75).

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.

* * *

Check out the new *Computer Security Handbook*, 4th Edition_ edited by Seymour Bosworth and Michel E. Kabay; Wiley (New York), ISBN 0-4714-1258-9. Available now at your technical bookstore or from Amazon < <http://www.amazon.com/exec/obidos/ASIN/0471412589> > and Barnes & Noble < <http://shop.barnesandnoble.com/textbooks/booksearch/isbninquiry.asp?isbn=0471412589> >.

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.

