Scavenging (2):
RAM and Virtual Memory

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

In this short series, we're looking at how to discard data safely.

The first area to look at is the least obvious: electronic storage. Data are stored in the main random-access memory (RAM, as in "This computer has 128 MB of RAM) in computers whenever the data are in use. Until the system is powered off, data can be captured through memory dumps and stored on non-volatile media such as CD-ROM. Forensic specialists use this approach as one of the most important steps in seizing evidence from systems under investigation. However, criminals with physical access to a PC or other computer may be able to do the same if there is inadequate logging enabled on the system. Furthermore, even if the system is powered off and rebooted, thus destroying the contents of main memory, most systems use virtual memory (VM) which extends main memory by swapping data to and from a reserved area of a hard disk. Examining the hard disk (usually with special forensic software) allows a specialist to locate a great deal of information from RAM such as keyboard, screen and file buffers and process stacks (containing the global variables used by a program plus the data in use by subroutines at the time the swap occurred). Although there is never a guarantee of what will be found in the swap file, rummaging around with text-search tools can reveal logon IDs, passwords, and fragments of recently active and possibly confidential documents. The most alarming aspect of swap files is that they may contain cleartext versions of encrypted files; any decryption algorithm necessarily has to put a decrypted version of the ciphertext somewhere in memory to make it accessible by the authorized user of the decryption key.

Physical protection of a workstation to preclude access to the hardware is the most cost-effective mechanism for preventing scavenging via the swap files as well as to reduce scavenging of disk-resident data. Tools such as secure cabinets, anti-theft cables, movement-sensitive alarms, locks for diskette drives, and special screws to make it more difficult to enter the processor card cage all make illicit or undetected access more difficult.

While we're on the topic of RAM, most handheld computers use RAM for storage. What happens when you have to return such a system for repairs? Users can set passwords to hide information on some systems (e.g., Palm Pilots) but there are lots of programs for cracking the passwords of these devices. If it is possible to overwrite memory completely, I recommend that the user do so before having the device repaired or exchanged. If the system is nonfunctional, administrators should decide whether the relatively low cost of replacing the unit is justified to maintain security. Old handheld computers make excellent and original coasters for hot or cold drinks; they can also be used as very short-lived Frisbees.

* * *

Participate in the Fourth Annual e-ProtectIT Infrastructure Protection Conference – 20-22 March 2002 at Norwich University in Northfield, Vermont. Full information at http://www.e-
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.