“Superzap” was an IBM utility that bypassed normal operating system controls. The term eventually became a generic word; with such a program, a user with the appropriate access and privileges could read, modify, or destroy any data on the system, whether in memory or on disk. Such tools can sometimes allow the user to avoid leaving an audit trail. Worse, normal application controls may be ignored; e.g., requirements for referential integrity in databases, respect for business rules, and authorization restrictions limiting access to specific people or roles.

What kinds of utilities qualify as superzaps?

- Privileged debuggers: tools which allow unrestricted access to memory and disk structures;
- Disk editors: permit any change to be written to disk without passing through the file system;
- Program patchers: modify executable program files without having to recompile source code;
- Database tools: can change portions of a database without regard for logical consistency;
- Spoolfile editors: modify output files before printing;
- Alternate operating systems: replace the normal operating system for diagnostic purposes.

In my own experience, I was told by one customer, a service bureau, that one of its customers regularly used a superzap program to modify production data. Other than warning the managers that such a procedure is inherently risky, there was nothing the bureau could do about it.

When I was running operations at a service bureau in the 1980s, I discovered that a programmer made changes directly in spoolfiles (spooled print files) on a monthly basis to correct a persistent error that had never been fixed in the source code. If such shenanigans were going on in a mere report, what might be happening in, say, print runs of checks?

So why tolerate superzaps at all?

Superzap programs serve us well in emergencies. No matter how well planned and well documented, any system can fail. If a production system error has to be circumvented NOW, patching a program, fixing a database pointer, or repairing an incorrect check-run spoolfile may be the very best solution as long as the changes are authorized, documented, and correct.
However, repeated use of such utilities to fix the same problems indicates a problem of priorities. Fix the problem now, yes; but find out what caused the problem and solve the root causes as well.

In the next issue of this newsletter, I’ll summarize some of the controls that can be applied to superzaps.

* * *


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.