Logic Bombs (2):
Bombs Away

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

In the first article in this series, we looked at logic bombs and time bombs installed by insiders.

It is very difficult to stop a determined inside attacker from modifying production code to install logic bombs. Preventing such bombs requires a thoroughgoing commitment to quality assurance and strict separation of duties. Here are some well-known principles for making the logic bomber’s task more difficult:

* Segregate operations from programming and testing.
* Institute a carefully controlled process for moving code into production.
* Only operations staff should have write-access to production code.
* Lock down your production code – source and executable – so that it is as close to impossible as you can get for unauthorized people (users, programmers, anyone) to modify programs.
* Assign responsibility for specific production programs to named positions in operations.
* Develop and maintain a list of authorized programmers who are allowed to request implementation of changes to production programs.
* Require authorization from the authorized quality assurance officer before accepting changes to production.
* Keep records of exactly which modifications were installed when at whose request.
* Use hash functions on entire files in the production library.
* Recompute all hashes against a secure table to ensure that no one has altered production files without authorization and documentation.
* Keep audit trails running at all times so that you can determine exactly which user modified which file and when.
* If possible, ensure that audit trails include chained hash functions. That is, the checksum on each record (which must include a timestamp) is calculated not only on the basis of the record itself but also using as input the checksum from the previous record. Modifying such an audit trail is much more complicated than simply using a disk editor to alter data in one or two records.
* Back up your audit files and keep them under high security.

For much more detailed analysis of how to safeguard production software, see the following chapters in the Computer Security Handbook, 4th Edition:
In the next of these four articles, we’ll look at logic bombs that are installed by consultants and at software license timeouts.

* * *

NEW! 18-month online Master of Science in Information Assurance offered by Norwich University; see <http://www.norwich.edu/msia> for full details.


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@norwich.edu>; Web site at <http://www.mekabay.com/index.htm>.

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.