Responsible Vulnerability Disclosure (1)

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

How should security vulnerabilities be disclosed by those who discover them? Should they be broadcast to everyone interested, including criminals? Should they be kept secret and sent only to the software creators? Should there be a time limit on how long product developers can be protected against disclosure? This issue, usually called “full disclosure,” has exercised security specialists, criminal hackers, and those in between for years.

For example, NTBugtraq’s moderator, Russ Cooper, enunciated his methods in 1999. His strategy is to reproduce the claims, then publish minor bugs immediately in the list. When he judges that bugs expose vulnerabilities with severe security implications, Cooper works with asks those reporting the bugs whether they want to work directly with the software developer (he calls them “Vendors”) to get a fix out before publication. However, he does allow immediate posting to the list by those who choose not to wait for a fix.

In November 2001, Cooper proposed “The Responsible Disclosure Forum” to formalize the process of vulnerability disclosure. He suggests a core group of about 1,000 security experts who would evaluate the significance of claimed vulnerabilities and promote timely correction of important problems. Another group, perhaps 50,000 volunteers, would receive a vulnerability advisory within 48 hours; the advisories might include methods for reducing system vulnerabilities even while waiting for fixes – all the while carefully avoiding details that might allow script kiddies to exploit the vulnerabilities.

***

In the next column, I'll report on additional responsible-disclosure initiatives from a group led by Microsoft and another by a group of security experts trying to work through the IETF.

***

For further reading:


***

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