In the previous column, I reported briefly on Russ Cooper's approach to responsible bug reporting. In this column, there are a couple of initiatives readers might find interesting.

* * *

In November 2001, Microsoft and a group of five security firms (@stake, Bindview, Foundstone, Guardent, and Internet Security Systems) worked with Microsoft at the Trusted Computing Conference to devise standards for responsible disclosure of security vulnerabilities. The proposals followed an essay by Scott Culp (manager of the Microsoft Security Response Center) in which he criticized indiscriminate publication of security-vulnerability details, argued that such disclosure had been instrumental in the development of dangerous e-mail-enabled worms, and called for self-restraint in such publication. The proposed guidelines floated by the six cooperating firms included a request for all publication of vulnerabilities to be delayed by at least 30 days to allow for time to develop, test and distribute patches. Critics argued that such a long delay would reduce pressure on Microsoft and other vendors to ensure adequate quality assurance before releasing new versions of their products.

In late 2001, Steve Christey (MITRE) and Chris Wysopal (@stake) circulated a preliminary draft of their Responsible Disclosure Process to colleagues before submitting it to the Internet Engineering Task Force (IETF) as a possible Request for Comment (RFC) in February 2002. Even though the document expired at the end of August 2002, this thoughtful proposal deserves attention from anyone interested in the full-disclosure problem. The authors propose detailed procedures and responsibilities for those who discover flaws and for those who can repair them.

Within a few weeks, the IETF turned down their proposal because, they said, human procedures fall outside the IETF’s purview. Such a claim seems to ignore long-established RFCs such as

* 1603 & 2418 (IETF Working Group Guidelines and Procedures),
* 1244 (Site Security Handbook),
* 2014 (IRTF Research Group Guidelines and Procedures),
* 2901 (Guide to Administrative Procedures of the Internet Infrastructure), and
* 3013 (Recommended Internet Service Provider Security Services and Procedures)

among others, all of which deal directly with human procedures relating to Internet technology.

Christey and Wysopal have stated that they will continue to work for acceptance of their proposals in other venues. In the meantime, readers may want to stay aware of developments in this important area of concern. Christey and Wysopal’s contact data are included at the end of their document and they have confirmed to me that they are happy to receive comments from interested parties.

* * *
In an upcoming column, I'll look at how software companies are responding to bug notifications – and how they ought to do so.

* * *

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.


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.