Gene Spafford Challenges Complacency

by M. E. Kabay, PhD, CISSP
Security Leader
INFOSEC Group
AtomicTangerine, Inc.

I would like to draw readers' attention to the remarks made by Prof. Eugene Spafford of Purdue University on the occasion of his receiving the National Computer Systems Security Award from the National Computer Security Center at the 23rd (and last) National Information Systems Security Conference in Baltimore, 16 October 2000.

On his biographical page at < http://www.cerias.purdue.edu/homes/spaf/ >, we read, "Gene Spafford is a Professor of Computer Sciences at Purdue University, where he has been on the faculty since 1987. His current research interests are primarily in the areas of information security, computer crime investigation and information ethics. He also has an appointment as a Professor of Philosophy at Purdue.

"Spaf (as he is known to his friends, colleagues, and students) is director of the Purdue CERIAS (Center for Education and Research in Information Assurance and Security), and was the founder and director of the (now superseded) COAST Laboratory. He is also the interim Information Systems Security Officer for Purdue University. Related to this, he is the founder and de facto director of the PCERT (Purdue Computer Emergency Response Team)."

In his plenary address to the Conference, Spaf made the following key points about the state of information security today (I am summarizing and paraphrasing Spaf's words):

* Security is going to get worse before it gets better because of human nature, including the people who design, write, deploy, use and abuse the systems – and even because of the people who guard the systems.

* Some software manufacturers have perceived security problems such as viruses to be someone else's problem.

* Scanning for viruses using known search strings doesn't work for everyone now because many people fail to keep their signature files up to date, but if we reach the projected 100,000 known viruses by 2004, there will be a new virus reported roughly every hour or two – and how will downloading signatures keep up with that threat?

* We are at risk in part because we have entrusted security to users who lack understanding and training in how to cope with the issues.

* Programmers and system administrators are inadequately trained, with enormous time wasted due to program and system crashes. In addition, known vulnerabilities remain unpatched on uncounted systems.

* Senior executives select software and hardware based on initial cost of acquisition instead of long-term operational costs and risk analysis. New features are assigned higher value than reliability.

*   The software industry, aware of the problems its members are causing, includes supporters of the UCITA [the Uniform Computer Information Transactions Act] which would help "shield themselves from consequences of shoddy practices, and even to prevent critical public comment on their wares. (I [Spaf] would strongly urge you to educate yourselves about the awful consequences if UCITA is passed in your states; see my [Spaf's] editorial in issue E38 of the IEEE Cipher as a starting point or refer to <http://www.4cite.org>.)"

Spaf issued the following challenges to everyone involved with information technology:

*   Commit to thinking about the foundations of security in software instead of patching fundamentally flawed systems.

*   Hold companies liable for bad products that fail because of faulty design and operation.

*   Stop ridiculing "stupid user tricks" and design systems to take into account the nature of people for whom computers are equivalent to appliances.

* Improve the education of computer programmers and others who will be involved in creating and managing systems.   Include human factors in students' education so they can address real-world problems.   Apply interdisciplinary perspectives.

* * *

Please see the page of information about the event at < http://www.cerias.purdue.edu/homes/spaf/ncssa.html > and read the full text of Spaf's remarks. Each one of his points is worthy of extended thought and discussion.

* * *

Mich Kabay can be reached by e-mail at <mkabay@atomictangerine.com>.   He invites inquiries about a wide range of information security courses and INFOSEC consulting services that he and his colleagues at AtomicTangerine would be delighted to deliver to your employees at your site and at your convenience.   For Web-based or CD-ROM online training in security from our INFOSEC University project, see < http://infosecu.com >.

For information about AtomicTangerine, visit < http://www.atomictangerine.com >.