From Product to Process: Bruce Schneier's Analysis of INFOSEC

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

Bruce Schneier is one of the intellectual giants of our field. Author of several books, including the much-translated and appreciated *Applied Cryptography* (see < http://www.counterpane.com/orderac2.html > to order his books), Mr Schneier has contributed many focused and insightful articles on fundamental aspects of INFOSEC. In particular, his free CRYPTO-GRAM newsletter, published monthly by his company, Counterpane Internet Security Inc., is always worth reading. See < http://www.counterpane.com/crypto-gram.html > for archives and subscription information.

In May, Crypto-Gram < http://www.counterpane.com/crypto-gram-0005.html > included the article, "Computer Security: Will We Ever Learn?"

Schneier opens with his oft-quoted dictum, "Security is a process, not a product." [A corollary is "Security is a process, not a state."] After describing known problems with operating systems and encryption algorithms, he asks, "Is anyone paying attention?" Alas, "the answer to this question is: not really. . . . No one is paying attention because no one has to." He explains that the lack of legal liability for incompetent software engineering lets manufacturers take the easy route of producing bad-quality security software. "Real security is harder, slower, and more expensive, both to design and to implement. Since the buying public has no way to differentiate real security from bad security, the way to win in this marketplace is to design software that is as insecure as you can possibly get away with."

I think that there have been efforts in the right direction to improve security products. My former long-time employer, ICSA Labs < http://www.icsa.net > , runs several industry consortia < > that focus on setting and applying standards of functionality and quality to different types of products. See < http://www.icsa.net/html/certification/ > for a description of the certification process at ICSA Labs. I know from personal experience with the consortia that the ICSA staff and the representatives from member companies take their job seriously. For example, the Anti-Virus Product Developers' (AVPD) Consortium raised the standards for anti-virus products very quickly so that the AVPDs could no longer compete on the basis of how many variants of malicious software they could identify: that information became common knowledge, and all of the participating anti-virus scanner products were tested against the same "zoo" and using the same test procedures. Within a few years, this quality-assurance effort paid off for everyone: users could count on effective anti-virus functionality from any ICSA-certified anti-virus product; AVPDs could focus on user documentation and interface, ease of installation, and frequency of updates rather than wasting time and effort futilely trying to win a numbers game.

Schneier recommends that everyone concerned with security keep track of known vulnerabilities using alert services and network vulnerability scanners. He argues that we ought to be monitoring all network components continuously. "Almost everything on your network produces a continuous stream of audit information: firewalls, intrusion detection systems, routers, servers, printers, etc. Most of it is irrelevant, but some of it contains footprints from successful attacks. Watching it all is vital for security, because an attack that bypassed one product might be picked up by another."

In a White Paper, "Managed Security Monitoring,", < http://www.counterpane.com/whitepaper.html > Schneier explains the results of his thinking: his company's focus on continuous monitoring of client security data as the heart of his company's business. He then describes in detail every element of the new service that his company is offering subscribers. As usual, the writing is clear and concise.

This is a marketing document that provides sound information and sound reasoning and therefore makes Schneier and his colleagues look good -- for real. I wish more companies would govern their marketing departments to ensure this kind of excellence in their documentation. If you have any sway over such people, why not slip them a copy of this column?

Finally, take a look at the information on Schneier's new book, Secrets and Lies: Digital Security in a Networked World on his Web site at < http://www.counterpane.com/sandl.html >. I am looking forward to getting a reviewer's copy from the author and will report my impressions in another column.

[Neither the author nor AtomicTangerine have a business relationship with Counterpane Systems and the above commentary is not to be construed as an endorsement of Counterpane Systems' services.]

* * *

Mich Kabay can be reached by e-mail at <mkabay@atomictangerine.com>. He invites inquiries about a wide range of information security courses he would be delighted to deliver to your employees at your site and at your convenience.

AtomicTangerine is the Internet's first e-business venture consulting firm, combining the disciplines of venture capital, technology innovation and strategic consulting to create category killers and incubate new industries for companies of all sizes and at all stages of evolution. AtomicTangerine headquarters are in the San Francisco Bay Area and we have offices in New York, London, Tokyo, Washington DC, Boston, Denver and Seattle/Tacoma. Visit our new Web site at <www.atomictangerine.com>.

limit on any Web site, and to republish it in any way they see fit.