INFORMATION SECURITY • A world of information for the security-conscious

SPECIAL FEATURE PROFILE

Designated Holist

A self-described "eclectical engineer," Peter Neumann brings balance to a field often characterized by chaos. **BY ANDY BRINEY**

There is much about Peter Neumann that is hard to figure. The man is a world-renowned computer scientist, a Harvard Ph.D. and Fulbright scholar who has spent the last 27 years working in the elite Computer Science Laboratory (CSL) at SRI International. He has done pioneering research on file system design and computer intrusion detection, testified before Congress on the perils of key escrow and sat on national infrastructure protection and Y2K committees. He moderates, *pro bono*, the wildly popular RISKS Forum, an electronic mailing list read by hundreds of thousands of Netizens around the world. In short, it s not a stretch to say that Neumann has helped revolutionize current thinking about such topics as system survivability, fault tolerance and risk avoidance.

Yet then you hear about the other half of Neumann the*right-brain* half. For recreation, he composes music, including compositions that, he says, "play themselves." He also plays several instruments, including the piano, bassoon, French horn and trombone. He can even play two recorders *at the same time*, in close harmony. He and his wife Liz were delighted to play in the 1998 "Tubafest," a Christmas music festival featuring 216 horns, all in the tuba family. Liz played the tuba, Peter the baritone horn.

Neumann also writes poetry and nonfiction essays, including one on the pros and cons of various abbreviations for "electronic mail": e-mail vs. email vs. Email vs. E-mail (conclusion: "The hyphen is desirable for *disambiguation*"). He kept his 1967 Ford Fair-lane wagon alive and running until 1997, fashioned together with plywood and duct tape. Once, he drove his friend and colleague Teresa Lund to the airport from SRI. "The thing shook and rattled and I was amazed we were able to get there safely," she says. Clearly, this is not your prototypical computer nerd.

Neumann s office in Menlo Park, Calif., is a perfect metaphor for the man. Located in the E building about 30 miles south of San Francisco, the room is a study in organized chaos. Bulging bookcases overflow with paper waterfalls, and stacks of reports, memos, journals and conference proceedings teeter on every square inch of desk space, including around and on top of his computer monitor (think *Shoe*). His friends say Peter never throws away *anything*; Peter, of course, says he knows exactly where everything is.

Nothing like a little earthquake to test such a claim. Sure enough, when a quake measuring 7.2 hit San Francisco in the fall of 1989, offices throughout his building were trashed. Desks and file cabinets toppled over, scattering books and papers into a messy free-for-all. Everyone expected Peter s office to look like a war zone. But legend has it that the towering paper stacks remained right where they were, not a paper clip or fax out of place.

The Forest for the Trees

As the office goes, so does the man. Peter Neumann is a pioneer and innovator in the field of information security precisely because he achieves balance in a field increasingly characterized by chaos. "I see myself as designated holist," he says, "in the sense that I m very often looking at the bigger picture when most folks are looking at very small details." A self-described "eclectical engineer" and "peregrine philosopher," Neumann approaches infosecurity as he does everything else as a single, albeit critical, component of a larger whole.

"Security is just one of the problems we ought to be dealing with. It s the old story of the man who loses his keys in a field somewhere, and he s looking for them under the light, because that s where the light is. Most people tend to try and solve problems in the small, and if you try to solve the security problem in the small, you don t get very far.

"If you look at a more difficult problem say, how do we develop survivable, secure, reliable systems and networks you

discover that there is a lot of commonality among the different requirements. There are things you can do much better if you address the more difficult problems first. This goes counter to the grain of, Just grab whatever s on the shelf and stuff it into your environment. That doesn t work very well when you re trying to develop very secure, very reliable, very robust systems. My role as designated holist is to look at this bigger picture."

Designated holist. Professionally, it s a role Neumann assumed early in his career, which took off in earnest in 1960 when he joined the Computer Science Lab at Bell Labs in Murray Hill, New Jersey. In 1965, Neumann helped design and develop Multics (Multiplexed Information and Computing Service), a mainframe timesharing operating system. Designed with security in mind, Multics introduced several novel solutions: hierarchically tree-structured directories, access control lists, symbolic file and I/O stream names, and dynamic linking, segmentation and paging, to name a few. Consequently, it was the first system to be awarded the B2 security rating by the U.S. government. Many of Multics s technological innovations are incorporated into the UNIX OS today; the name "UNIX," in fact, is a pun on "UNICS," a singular form of "Multics."

Light-years ahead of its time in terms of security, Multics also brought to the surface a unique problem with two-digit date fields the basis of the Year 2000 problem plaguing the globe today. In Multics "we recognized and avoided the Y2K problem 35 years ahead of time," he says. "It was obvious even then: Why build a system that s not going to go into the future?"

The Jewel of IDS

Back before SRI banned smoking on the premises, legend has it Peter would put on a gas mask if someone lit up in a meeting. Today he devotes a lot of effort to seeing through the haze surrounding modern approaches to system survivability, including computer intrusion detection.

Neumann s research into anomaly and misuse detection took off in the early 80s with the development of the Intrusion-Detection Expert System (IDES), the first of a five-generation system that has laid the groundwork for most commercial IDS products in use today. IDES and its successor NIDES (Next-Generation Intrusion Detection Expert System) were the first to use both signature analysis and anomaly detection, thereby addressing the need for a flexible approach to user-oriented monitoring and profiling in real-world computing environments.

"The challenge was to work not just for a bunch of known scenarios or known attack modes, but to be able to detect unanticipated failure modes and new penetrations that nobody s ever discovered," Neumann explains. "So the statistical stuff is intended to look at deviations from expected, normal behavior. And the role-based or signature-based stuff is intended to look at the known scenarios. We re trying to generalize all of this to security as well as to survivability in a general sense."

Limitations in NIDES s scalability and interoperability paved the way to Neumann s current research project: EMERALD (Event Monitoring Enabling Responses to Anomalous Live Disturbances), a DARPA-sponsored project he is working on with CSL s Phillip Porras. Unlike NIDES, EMERALD extends to the network level and integrates into distributed computing environments, enabling hierarchical interpretations of distributed monitoring units and cross-platform analysis at various layers of abstraction.

Technologically, EMERALD uses advanced software engineering techniques in an attempt to solve the more difficult problems: generality, flexibility, system independence and long-term evolvability. "The work at SRI, including EMERALD, has always been instrumental in guiding and influencing research in intrusion detection," says Paul Proctor, chief technical officer at Centrax Corp., a San Diego-based network security outfit.

In talking to Neumann, however, you get the sense that he s less excited about EMERALD s technology than its potential as a research prototype. In addition to building an accompanying set of exportable APIs to facilitate interoperability between EMERALD and other network monitoring facilities, CSL is working on a free version of the expert system that could be put up on SRI s Web page for teaching purposes. In effect, this would allow others "to write rules to detect various types of misuse using our expert system technology in a collaborative way," Neumann says.

The key concept here is *collaboration*. For in EMERALD Neumann has achieved not only a high-water mark in intrusion-detection methodology, but a prototype of a *robust* open-source (ROS) system the next logical step in the software industry s fledgling open-source movement. This, he says, is his larger calling, the place where his professional pursuits meet his personal, "big-picture" worldview.

"In my old age, I m getting less interested in excruciating detail, which I once did as part of my life. Certainly in the Multics days, there was a lot of detail. Now I m involved in designing and dealing with systems that are intended to be much more

robust than off-the-shelf stuff." The challenge is huge: to extend the robust open-source effort beyond EMERALD and beyond the study of intrusion detection indeed, even beyond the field of information security itself. His goal is no less than laying the groundwork for the robust open-source movement throughout the field of software engineering.

Neumann characterizes the effort as "a *very* important opportunity for the future." But he is also realistic about the practical aspects of such a monumental project, and so his first step was to enlist the help of others through an electronic distribution list. The project is still in its formative stages, and Neumann won t discuss who is on the list or where they are in the discussions ("I don t want a monster here," he says). But he does have concrete ideas about the larger purpose of the project. In a "prolegomenon" circulated to select colleagues, he writes,

> *We seek open-source systems and subsystems that have a much better chance of avoiding the myriad risks that we now have to live with. It is certainly not aimed at perfect systems, because there are no such systems and never will be. However, it is aimed at creating an environment that encourages an international, collaborative, integrative process by which highly interoperable components can be evolved from scratch when necessary, but otherwise from less robust components that exist today and that continue to be improved and then subsequently readily composed into systems and networks capable of ever-greater robustness.*
>
> *The entire process needs to be open-ended, long-term, far-sighted and incremental . There are already very substantive efforts to develop, maintain and support open-source software systems. We hope that all of these efforts will be participants in what could become a mainstream, integrative Robust Open-Source (ROS) movement, not just a countercultural outlier (ROSwell?). If it succeeds in producing demonstrably robust systems, it might even have an influence on some of commercial systems whose developers are open-minded enough to embrace it. But if that does not happen, the expectation is that a large body of interoperable systems and subsystems could nevertheless emerge.*

The ROS effort, Neumann concludes, will require "a certain amount of altruism" and "an almost religious-zeal commitment." Which makes you wonder: Who better to lead the cause?

Catbird s Seat

Back at his office at SRI, between the bookcases and amid the stacks of paper, Neumann has a reproduction of a Paul Klee painting hanging on the wall. The picture is of a cat contemplating a bird sitting on its forehead. For a man whose life is full of metaphors, this one seems the most appropriate. For while he is content with the balance he has struck between his professional and personal pursuits the left brain and the right, working as one he never stops thinking about possibility, about "What if ?"

"The beauty in life, the wonderful challenge," he says, "is to find things that really make you happy with what you re doing. I m very happy with the balance of things I m doing. But it s always important to keep learning."