Security and Source-Available Systems: Risks and Opportunities

Peter G. Neumann, Session Chairman
Computer Science Lab, SRI International, Menlo Park CA 94025-3493 USA
National Information Systems Security Conference NISSC 2000
16-20 October 2000

We must do a better job of developing robust systems and applications that can satisfy serious requirements for security, as well reliability, human safety, and survivability in the face of a wide range of realistic adversities—including hardware malfunctions, software glitches, inadvertent human actions, a wide range of attacks, and environmental problems. Ideally, these systems should be interoperable, evolvable, easily managed and operated, and maintainable.

Today's mass-market proprietary closed-source software seriously impedes efforts to improve installed systems in response to recognition of new vulnerabilities and risks. Source-available software—for example, from the Open Source (http://www.opensource.org) and Free Software (http://www.gnu.org) movements—provides a potential alternative, enabling open collaborative efforts, widespread review of source code, rapid generation and acquisition of fixes, and a broad community of collaborators. Additional benefits also accrue from well-defined open requirements and open specifications.

There are of course risks that your attackers can find and exploit your flaws before you do. However, security by obscurity is clearly a flawed philosophy, despite the fact that security is often reduced to that approach—which may be why it fails in the light of weak operating systems and networking.

This panel will explore the source-available alternatives and how they might best contribute to the development and operation of meaningfully robust secure systems.

See http://www.csl.sri.com/neumann/ieee00+.ps and .pdf for some background on robustifying open-source systems.

Dr. Peter G. Neumann <neumann@csl.sri.com> is a Principal Scientist in the Computer Science Laboratory at SRI (where he has been since 1971), concerned with computer system survivability, security, reliability, human safety, and high assurance. He is the author of *Computer-Related Risks*, Moderator of the ACM Risks Forum (comp.risks), Chairman of the ACM Committee on Computers and Public Policy, and Associate Editor of the CACM for the Inside Risks column. He is a member of the U.S. General Accounting Office Executive Council on Information Management and Technology. See http://www.CSL.sri.com/neumann/ for Senate and House testimonies, reports, RISKS, papers, slides, etc. Neumann is a Fellow of the American Association for the Advancement of Science, the ACM, and the Institute of Electrical and Electronics Engineers (of which he is also a member of the Computer Society). He has received the ACM Outstanding Contribution Award for 1992, the first SRI Exceptional Performance Award for Leadership in Community Service in 1992, the Electronic Frontier Foundation Pioneer Award in 1996, the ACM SIGSOFT Distinguished Service Award in 1997, and the CPSR Norbert Wiener Award for in October 1997, for "deep commitment to the socially responsible use of computing technology."

Jay Beale is the Lead Developer of the Bastille Linux Project (http://www.bastille-linux.org). He is the author of several articles on Unix/Linux security, along with the upcoming book "Securing Linux the Bastille Way," to be published by Addison Wesley. At his day job, Jay is a security admin working on Solaris and Linux boxes. You can learn more about his articles, talks and favorite security links on-line (http://www.bastille-linux.org/jay).

Dr. Crispin Cowan is the CTO of WireX Communications, Inc., and is a Research Assistant Professor at the Oregon Graduate Institute, where he teaches a graduate course in system security. His research focuses on making existing systems more secure without breaking compatibility or compromising performance. Professor Cowan has authored 28 refereed publications, including those describing the StackGuard compiler for defending against buffer overflow attacks, and an invited talk at SANS 2000 dissecting buffer overflow attacks and defenses. Professor Cowan has been on the program committee of the USENIX Security Symposium, is the publicity chair for the New Security Paradigms Workshop, and is on the editorial board of the SANS Newsbites.

Eric Raymond is one of the prime movers in the Open Source movement. See <http://www.tuxedo.org/~esr/press.html> for bios and <www.opensource.org> for background.