Foreword

“There is more to life than increasing its speed.” This aphorism by Mohandas K. Gandhi can be applied to computing technology as well as one’s life: there is more value to it than simply increasing its speed. There are measures of worth other than those of speed and cost, and this book is an introduction to thinking about them, particularly in the context of security and privacy.

It is possible to view technologies as having multiple “waves” of development. The first such phase is to explore what may be accomplished with the new technological innovation. Whether we think about development of steam power, lasers, computing, or nanotechnology, there is a clear surge of effort by researchers and hobbyists to discover what might be done with the new technology. When some of the fundamental uses and bounds are discovered, a second wave begins as there are attempts to make the technology more reliable and consistent. This involves development of fault tolerance, standards, safety mechanisms, and understanding operational envelopes. Thereafter, a third phase is seen that is directed to making the technology more deployable: cheaper, smaller, and simpler to use, usually in a commercial context.

These three phases are visible when examining the history of almost any major technology. For instance, the airplane went from “we can fly” to “we can fly each time without crashing” to “we can mass-produce planes to use in commerce.” Think about the evolution of transistors from a lab bench in Bell Labs, to integration into ICs, to quintillions of transistors on bits of silicon manufactured around the world. Or consider the transition of lasers from a room full of components to DVD players and presentation pointers, or the development of the automobile from first horseless carriage to modern hybrid vehicle. There is an evolution of each technology that includes these first three waves.

So too, computing has passed through these three phases. The first phase is still occurring but might have reached its peak in the 1970s through the 1990s as scientists and engineers explored what was possible to do with computing and information technology. We discovered foundations of operating systems, language grammars, networking, database, encryption, and more. From the 1980s through the near future we have been observing the second phase, as standards have been developed for protocols and interfaces, fault tolerant computing and storage (e.g., RAID) is explored, and new security mechanisms developed to “harden” the interfaces for internet commerce. There has been a near simultaneous third phase as new methods have been developed to reduce the size and cost of the technology, both hardware and software, to the point where the aggregate embedded computing in a modern kitchen or new automobile comprises more processing power and storage than was present in the entire world 50 years before — at a cost reduction of more than seven orders of magnitude.

We are now in a fourth phase of technology development, the one implied by the Mahatma’s saying: the consideration of how the technology affects the quality of human life and dignity. Technology can change the way we live, alter economic and social balances, and change our abilities to achieve — but as sweeping as those changes may be, they do not necessarily occur without problems.

Computing and information technology can improve the world with increased access to information, better communication, and increased efficiency of large systems. We can enhance lives with on-line education and computer-controlled medical implants. However, we can also destroy privacy with unchecked data collection and correlation, and endanger whole economies with cyber attacks on critical infrastructure. For every bit of information that is gained to enhance our enforcement of laws we may also be reducing the privacy of those who are protected by those laws. New methods devised to protect a system from unauthorized use might also be used to suppress free speech and justified dissent.

It is important that those who are involved with the development and deployment of new cyber technologies understand these effects and tradeoffs. Science and the pursuit of knowledge may or may not be morally neutral, but the utilization of that knowledge in deployed technology has associated issues of ethics, policy, and law that the technologists ignore at their (and our) peril. The issues are more than science and engineering because people and societies are also involved: there are issues of law, of political science, of economics, of philosophy, of psychology, and more. The problems encountered in ensuring that systems are used appropriately are problems that cannot be solved with technology alone, but neither are they problems that can be addressed independent of the underlying computational fabric. Instead, they require an informed, multidisciplinary approach.

Nowhere is this approach more important than when considering issues of security, privacy, assurance, and crime. These are fundamental issues that computing and information technologies affect in overt (and sometimes, surprisingly subtle) manners. Recent history has shown how cyber crime and misuse can affect the world, both on the scale of nations and of individuals. Whether it is part of a military action against a country, such as Georgia, or the violation of a single individual's email privacy, computing technology can have a long-lasting and profound impact.

CERIAS (the Center for Education and Research in Information Assurance and Security) at Purdue University was founded in 1998 with the explicit mission of addressing these multidisciplinary issues in computing and information technologies. The editor of the book you are now reading, Professor Melissa Dark, has been an integral part of the Center from near its beginning, and she has a keen understanding of the need for a broad perspective on issues and approaches to addressing some of the fundamental challenges posed in this field. Guided by that experience, she has collected this volume of essays to expose some of the most important challenges — and approaches to their solutions — posed by the ever-increasing use of information technology.

No set of static readings can solve the total set of cyber security and privacy issues we face now and will face in the future. To really address those challenges will require ongoing efforts by a wide range of experts. Thus, it is critical that the computing experts, in particular, are familiar with the basic issues, understand some of the multidisciplinary nuances, and are able to engage the right communities in finding solutions to the most pressing problems. This book is intended to address that need for understanding. The material in this book should be considered as fundamental in any cyber curriculum as complexity bounds on algorithms and calculating throughput on a network; complexity bounds on algorithms and throughput analyses can increase the speed of our computing, but to paraphrase the Mahatma, there is much more to computing than increasing its speed. So, read these essays slowly and carefully, and consider, along with the authors, how computing should change the world for the better.

Eugene H. Spafford
Purdue University, USA

Eugene H. Spafford *has been working in computing for over 30 years, with activities in cyber security for most of that time. Spaf's (as he is known by many) current research interests are focused on issues of computer and network security, cyber-crime and ethics, and the social impact of computing. He is the founder and executive director of the Center for Education and Research in Information Assurance and Security (CERIAS) at Purdue University. This university-wide institute addresses the broader issues of information security and information assurance, and draws on expertise and research across all of the academic disciplines at Purdue. Spafford has received recognition and many honors for his research, teaching, and service, including being named as a Fellow of the ACM, of the AAAS, the IEEE, the (ISC)^2, and as a Distinguished Fellow of the ISSA.*