Editorial

Steve J. Chapin

Systems Assurance Institute,
Department of Electrical Engineering and
Computer Science, Syracuse University,
Syracuse, NY 13244, USA
E-mail: chapin@syr.edu

Biographical notes: Steve J. Chapin is an Associate Professor of Computer Science at Syracuse University, Syracuse, New York, USA. He holds MS and PhD Degrees from Purdue University. He has published more than 50 papers in the areas of distributed systems, resource management, networked quality of service, reliability, protocol steganography, application security, and system security. He is the Founding Director of the Systems Assurance Institute at Syracuse University, a university-wide institute focusing on interdisciplinary research and education in assurance issues spanning the areas of science, engineering, technology, management, public policy, communication, and law.

Assurance – the correctness, reliability, availability, safety, and security – of information and information infrastructures is crucial for the economic well being of commercial enterprise and international security. The explosive growth of the Internet from the 1980s through today has led to the deployment of inter-networked information systems of continuously growing complexity. Nearly every major business and government branch, including the military, has increased, and will continue to increase, its dependence on the Internet for day-to-day operations. Currently, without heroic measures, we are unable to assure that our information systems will behave correctly, reliably, or safely, nor are we able to guarantee availability or security.

Systems assurance goes beyond traditional computer security in that it considers the users, policies, laws, and technology as a cohesive whole. Focusing solely on technology does not provide assurance, for history has shown repeatedly that technology without proper policy and education does not make systems secure. Education alone will not suffice: even users who know better choose weak passwords, use them across many systems, share them with others, and do not change them regularly. Policy (both public and private), in the absence of an understanding of the underlying technologies and the people who use them, will only create confusion and disdain. In short, no one discipline can produce assured systems in isolation – it is through the application of holistic solutions comprising elements from all these disciplines (and more) that we will produce systems that are secure, reliable, usable, and trustworthy.

The five papers contained in this special issue are diverse in their treatment of assurance. The topics covered range from high-level concepts of accountability in business organisations, to notions of trust in dynamic routing for mobile ad-hoc networks, to more traditional technical subjects such as reputation frameworks for peer-to-peer applications, distributed checkpointing, and intrusion-tolerant database

systems. These topics touch on the breadth of the area, but are by no means exhaustive. The limited space available prevented us from publishing other papers on topics such as role-based models of trust and authority, and applications of cryptography in grid security. We expect that those papers will appear in future issues of this journal.

I would like to thank the authors who submitted papers, the referees who reviewed them, and the Editor for their collective assistance in producing this special issue. I very much appreciate the patience and support throughout the publication cycle, and thank them for the opportunity to bring their work to you.