In July 2014, the Charles Babbage Institute (CBI) hosted a workshop sponsored by the National Science Foundation (NSF) on the history of computer security, which resulted in the April–June 2015 “Computer Security” special issue of the *Annals*. This issue is the second special issue extending from that workshop. It includes two articles by the event’s co-organizers (Thomas Misa and myself) and a revised paper from the workshop by William Aspray (University of Colorado) and James W. Cortada (CBI). It also includes an article we recruited by Bradley Fidler (University of California, Los Angeles) and Quinn DuPont (University of Toronto).

We are grateful to the NSF—and particularly Secure and Trustworthy Cyberspace (SaTC) program officers Carl Landwehr and Jeremy Epstein—for supporting (and attending) the workshop as well as funding a major four-year CBI research effort to build infrastructure for the history of computer security through oral histories, archival collection, publications, and a computer security wiki. Since the 2014 workshop, we have conducted and published 31 oral histories, added many important collections, and published these two *Annals* issues. I am also writing a book under contract with MIT Press (tentatively titled “From Time-Sharing to the Cloud: A History of Computer Security”) in this area, and our wiki has received wide use.

In this issue, Misa’s article explores the origins of the multilevel computer security problem by focusing on research and systems at the RAND Corporation, System Development Corporation (SDC), and the National Security Agency (NSA). The 1970 (Willis H.) Ware Report and the 1967 Spring Joint Computer Conference (SJCC) Ware-led “Computer Security and Privacy” session are focal points of historians and computer security scientists and are generally considered the beginning of multilevel computer security. However, Misa shows that prior to the Ware Report, pioneering time-sharing systems by SDC (Q-32) and NSA (RYE) were designed and developed. These early-to-mid 1960s systems and their implementations represented the true start (in the classified community) to confronting the multilevel computer security problem. In fact, they informed the well-developed understanding of it that insiders Ware and the NSA’s Bernard Peters displayed at the SJCC session.

Symantec has long been a leading company in computer security products and services. Aspray and Cortada’s article focuses on the early years of this company founded in 1982 by Gary Hendrix (a former scientist at SRI) to develop artificial intelligence software applications. They detail the firm’s strategic evolution as it investigated and engaged in R&D and acquisitions in a number of different areas of software applications. The case offers a rich examination of venture funding, inca- tion, and merger and acquisition activity in the early personal computer software industry. In 1990 Symantec acquired Peter Norton Computing, which soon led it to focus on antivirus software as well as other areas of computer security and data management.

Much of computer security has focused on access control technologies and standards to keep unauthorized individuals and malware out of computer systems. Alternatively, my article, “The March of IDES,” concentrates on the history of intrusion detection expert systems, or automated batch and real-time audit tools to detect intruders or malware. It examines the first influential system, which took the name that defined its type—SRI’s Intrusion Detection Expert System (IDES)—as well as its successor NIDES. The article also discusses NSA’s Computer Misuse and Anomalies Detection research program and the disproportionately strong leadership contributions of women scientists to the intrusion detection system field.
Lastly, DuPont and Fidler provide an important history of Private Line Interface, a cryptography computer security tool developed under DARPA-sponsorship by Bolt, Beranek and Newman for use on the Arpanet. They show how PLI—which operated between network switches and host computers—was at the “edge” of the network. They demonstrate how this set a pattern for network cryptography tools existing at the edge of networks, including the Internet, and how these developments have helped shape conceptions of contemporary cybersecurity.

Jeffrey R. Yost is the associate director of the Charles Babbage Institute (CBI) and a faculty member in the History of Science, Technology, and Medicine at the University of Minnesota. He is a former editor in chief of IEEE Annals. His primary areas of research are the business, social, and cultural and intellectual history of information technology. Yost has a PhD in the history of technology and science from Case Western Reserve University. Contact him at yostx003@umn.edu.