Computer Security

Jeffrey R. Yost
Charles Babbage Institute

Few areas of computing capture more headlines today than cybersecurity. Yet, historians have barely scratched the surface of the rich history of computer security due in large part to lack of relevant archival and other source materials. With encouragement from computer-crime expert Donn Parker, in early 2011 Thomas Misa and I proposed to the National Science Foundation (NSF) a multiyear Charles Babbage Institute (CBI) computer security history infrastructure project. NSF Trustworthy Computing Director Carl Landwehr funded this project (NSF 1116862), which is now overseen by his successor, Secure and Trustworthy Cyperspace (SaTC) Director Jeremy Epstein. In addition to Landwehr and Epstein, we are grateful to the computer security pioneers who serve on our project's advisory board: Rebecca Bace, Matt Bishop, Bob Johnston, Stuart Katzke, Steve Lipner, Andrew Odlyzko, Donn Parker, and Gene Spafford.

The CBI project consists of conducting 30 research-grade oral histories, collecting archival resources, developing a computer security wiki, and publishing original scholarship. We have made major advances on all fronts, having conducted oral histories with 26 seminal figures (to date) in computer security (including Rebecca Bace, David E. Bell, Peter Denning, Dorothy Denning, Butler Lampson, Carl Landwehr, Karl Levitt, Steve Lipner, Teresa Lunt, Peter Neumann, Roger Schell, and Gene Spafford), secured important new archival collections (from Steve Lipner and Lance Hoffman), produced a frequently visited wiki,[1] and published scholarship.

With our project's core being "infrastructure," or facilitating scholarship by ourselves and others, we proposed to NSF an add-on Computer Security History Workshop of historians and pioneers held at CBI in July 2014 (a write-up appeared in the January–March 2015 issue of the *Annals*[2]). This issue is the first of two special issues of the *Annals* publishing the revised papers from that workshop. It markedly advances scholarship on many different critical aspects of computer security history.

Michael Warner and Steve Lipner's articles focus on important foundations of computer security and their aftermath. Warner concentrates on policy history within the legislative and executive branches. He highlights key policy responses to potential foreign threats to US government information systems between the mid-1960s and the early 2000s. Lipner examines the context and challenges with implementing computer security standards (with a goal of commercially produced "high assurance" systems) under the Department of Defense's Trusted Computer System Evaluation Criteria (TCSEC), or the Orange Book. It turned out that lengthy and costly system development and unwieldy certification hindered the goal of commercial high assurance systems, leading to the "death" of the Orange Book in favor of the "more straightforward and deterministic" international Common Criteria in the 1990s.

My article and Rebecca Slayton's each extend these foundations. I examine the importance of IBM user group Share and how IBM and start-up SKK listened to organizational users and built access control systems (short of high assurance) that were widely purchased by companies and launched the computer security software products industry. Slayton examines computer security metrics used by the US government where regulators placed a high value on risk analysis while practitioners questioned the measurement of risk. She demonstrates that the value of risk analysis was often overlooked, even as it led to important individual and organizational learning.

 Published by the IEEE Computer Society 1058-6180/15/$31.00

Finally, Laura DeNardis and Dongoh Park focus on aspects of the political and social history of digital communication security, surveillance, and cryptography. DeNardis analyzes the design tension between national security interests for surveillance and network security in computer networking from the mid-1980s into the 2000s, concentrating on the work of the Internet Engineering Task Force (IETF). She demonstrates how the Internet engineering community has consistently opposed indiscriminate technologically based government surveillance. Park's article provides a case study of public-key encryption technology in South Korea. He details how US export regulations on cryptographic technology led the Korean government to develop identity infrastructure consisting of a unique public-key encryption algorithm. His case highlights the major social and cultural challenges, as well as technological ones, in implementing a PKI system.

Reference and Notes

1. See https://wiki.umn.edu/CBI_ComputerSecurity/.
2. T.J. Misa, "CBI–NSF Computer Security History Workshop," *IEEE Annals of the History of Computing*, vol. 37, no. 1, 2015, p. 83.

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.

From the Editor in Chief

It is a great pleasure to welcome back to the *Annals* as guest editor of this special issue Jeffrey Yost, who served as the editor in chief of the *Annals* from 2008–2011. This past summer, Jeffrey was also one of the organizers of a conference on computer security sponsored by the National Science Foundation (NSF) and hosted by the Charles Babbage Institute. Out of this extraordinarily productive conference came the series of articles that comprise this first of two planned *Annals* special issues on computer security. The collection of articles that Dr. Yost has selected for this issue highlight the wide range of perspectives that were represented at the conference, which included not only academic historians, but also security pioneers, industry practitioners, and policy experts. I have been a participant at several similar events in which it was hoped that a diverse and interdisciplinary group of contributors would produce novel and illuminating exchanges, but never one that was so successful in accomplishing its agenda. This is a testament to the hard work that Jeffrey Yost and Thomas Misa put into organizing the conference, and for this, the community of historians of computing thanks them.

As Jeffrey points out in his own introduction to the special issue, computer security is not only one of the most active and intellectually exciting areas of contemporary computer science research, but it also one that has social, political, and economic dimensions that make it interesting and relevant to a broad audience of nonspecialists. I am particularly pleased, therefore, that with this special issue the *Annals* can help to open up a new field of historical inquiry that will no doubt become an increasingly significant topic for computer historians, policy makers, and the public alike.

—Nathan Ensmenger