Review of the book

"The History of Information Security - A Comprehensive Handbook"
by Karl de Leeuw and Jan Bergstra (editors),
Elsevier
2007

ISBN: 0444516085, 978-0444516084

Ross Anderson
University of Cambridge, Computer Laboratory

This magisterial book, of almost 900 pages, has joined Kahn, Yardley and Welchmann on my shelf of serious reference works. Yet it contains much that I found new, surprising and even delightful, despite a quarter century of working in the field.

The book's strength is its scope, both in subject matter and in historical perspective. Its 29 chapters include one by Whit Diffie and Susan Landau on the export of cryptography in the 20th and 21st century, but also one by the historian Eddie Higgs on the history of identification in England from 1475. (Declaration of interest: I met the editor at a delightful workshop that Eddie organised at Oxford on this subject.) A historical perspective can remind us of the many and changing contexts of authentication systems, from centralizing power and supporting religion through containing welfare costs and catching army deserters to defining the very essence of citizenship.

Engineers will be pleased to see chapters on such topics as the history of biometrics, document security, rotor machines and computer crime. Too many computer scientists reinvent things; it could be really useful to a student working on biometrics, for example, to read of the pioneering research that was done on recognising fingerprints, faces, speakers and signatures back in the 1960s.

Crypto historians will enjoy substantial chapters on crypto in the Renaissance and the Dutch republic, and a chapter on the emergence of the first "information society" in eighteenth-century Britain. This period saw not just the Enlightenment and the industrial revolution, but the forging of the first modern state, combining not just capitalism, democracy and the rule of law, but news management and postal interception; a weak state redirected surveillance from foreign diplomats to domestic suspects. Most other states have followed the eighteenth-century British model - aping its vices as well as its virtues.

The more modern history of crypto includes chapters on Boris Hagelin and Crypto AG; on Tunny and Colossus; and on KGB sigint during the Cold War. Unfortunately the Crypto AG history was written by one of its staff, and does not mention the Buehler case; but the KGB history does contain some nuggets, including the poverty of Soviet human intelligence resources by the time of the Cuban crisis and the huge increase in sigint investment authorised by the Kremlin to offset this. The cold-war USA and USSR may have been more similar in their intelligence posture than has previously been realised.

Other chapters range from limitations on scientific publication, through the history of the Orange Book and other information security standards, to a final chapter on how warfare is being transformed by the information revolution.

Overall I found this book a goldmine—a valuable addition to my library. In a business like ours, which depends on the interaction between technology that changes and human nature that doesn't, it's all too easy ignore historical lessons. De Leeuw and Bergstra's book is a worthy antidote. It's also useful that the authors come from a wide range of backgrounds, from engineers and historians to lawyers and social theorists; a diversity of perspectives also matters.

The reviewer is Professor of Security Engineering at Cambridge University Computer Laboratory.