Review of the book

"Security Engineering – A Guide to Building Dependable Distributed Systems, 2nd edition"

by Ross Anderson

John Wiley & Sons 2008

ISBN: 978-0-470-06852-6

Safuat Hamdy
Secorvo Security Consulting GmbH, Karlsruhe, Germany

August 12, 2010

1 What the book is about

This review describes the second edition of Ross Anderson's book *Security Engineering*. Summarising the content, this book describes the interaction between security, engineering, human psychology, and usability; it covers the security pitfalls due to non-engineering aspects that engineers use to step in. Following Anderson, so far cryptographers have talked only to other cryptographers, systems people only to other systems people, engineers only to other engineers, and so on. However, security spans a whole lot of scientific disciplines, and as long as folks from one discipline doesn't talk to folks from other disciplines, there is no way to get security right as a whole. This book tries to bridge the gaps. As this seems to be one of Andersons favourite topics it is not surprising that the second edition is almost twice as voluminous as the first edition, and Anderson leaves no doubt that the second edition will not be his final word on that.
The first edition is freely online available at `http://www.cl.cam.ac.uk/~rja14/book.html`, where you find also some sample chapters from the second edition. Like the first edition, the second edition is brought to you in three parts; however, Anderson has added, renamed, and removed a few chapters. The following will summarise the content of each chapter and the major changes in comparison to the first edition.

Chapter 1 – What is Security Engineering? This introductory chapter on security engineering sets the stage, provides some sample scenarios and defines a few terms as they will be used in the book throughout. Compared to the first edition, there have been relatively few additions and extension.

Chapter 2 – Usability and Psycholgy This chapter describes the interaction of security engineering with aspects of usability and psychology. Topics included are attacks based on human behaviour such as phishing, aspects of psychology, passwords, and system issues such as attacks on how users interact with machines. This chapter supercedes Chapter 3 on Passwords from the first edition; compared to the first edition this chapter has been substantially expanded.

Chapter 3 – Protocols In this chapter Anderson discusses various security protocols and attacks on them with focus on authentication. He introduces BAN logic, demonstrates how it works, and discusses its limitations. This chapter has received only few additions; the most notable change is a new section on practical key management.

Chapter 4 – Access Control This chapter is one of the more technology specific chapters and thus is naturally a candidate for an overhaul. For instance, the windows specific details have been lifted to Windows Vista, while aspects of OS/X have been newly included. Also new is a general discussion on middleware issues as well as aspects of sandboxing and virtualisation.

Chapter 5 – Cryptography This chapter gives a rough introduction on cryptography for those who don't need to understand the gory details of cryptography. Except a few minor updates and additions this chapter is identical to the accordant chapter of the first edition.

Chapter 6 – Distributed Systems This chapter discusses the security relevant aspects of concurrency in a network such as time, order, and state. This is followed by a discussion on fault tolerance and issies of naming. This chapter has received more explanations but is otherwise idebtical to the chapter from the first edition.

Chapter 7 – Economics This chapter discusses the economical incentives to security or insecurity. This chapter is new in the second edition.

Chapter 8 – Multilevel Security Here the reader finds the classical topics like Bell-LaPadula or Biba. The section on future MLS systems has been much expanded; topics include now the according mechanisms of Vista, Linux and SELinux, and virtualisation. Apart from that, the difference to the chapter in the first edition is more text.

Chapter 9 – Multilateral Security This chapter covers another classics, namely compartmentation, the Chinese-Wall model and the BMA model. The other major contribution of this chapter is the discussion of problems of inference and possible strategies to deal with that. This chapter is basically identical to that from the first edition.

Chapter 10 – Banking and Bookkeeping This chapter covers classics such as double-entry bookkeeping and the Clark-Wilson Security Policy Model. The first part of this chapter coincides with the accordant chapter in the first edition. The major addition are extensive sections on credit cards and fraud detection, smartcard-based banking and EMV, and home banking.

Chapter 11 – Physical Protection This chapter covers plain physical security mechanism such as walls, barriers, locks, and alarms. The chapter consist of major parts of the chapter on monitoring systems in the first edition, supplemented with a lot of updates and new text.

Chapter 12 – Monitoring and Metering This chapter is devoted to physical metering systems such as utility meters, taximeters and tachographs. This chapter is in essence the second half of the chapter on monitoring systems from the first edition.

Chapter 13 – Nuclear Command and Control The highlights of this chapter are shared control schemes and treaty verification (tamper resistance is introduced as well but dealt with in much greater detail in a later chapter). This chapter is in essence unchanged compared to the first edition.

Chapter 14 – Security Printing and Seals This chapter highlights another physical security mechanism; various issues such as techniques and limitations are being discussed. In essence the same as in the first edition with a few updates.

Chapter 15 – Biometrics Here the reader will find the discussion of classical topics such as fingerprints, face and voice recognition, handwriting and other techniques of biometrics. In essence the same as in the first edition with a few updates and more explanatory text.

Chapter 16 – Physical Tamper Resistance In this chapter Anderson discusses physical smartcard security. Specifically, various techniques and their limitations are being discussed. In essence the same as in the first edition with various updates and more explanatory text.

Chapter 17 – Emission Security In this chapter issues around the emission of electromagnetic signals are being discussed, but other side channels are also being discussed. Topics include passive attacks such as simple wiretapping and power analysis as well as actice attacks such as differential fault analysis. Apart from updates this is the same as in the first edition.

Chapter 18 – API Attacks This short chapter deals with security issues around programming interfaces; the focus is on APIs of security modules. This chapter is new.

Chapter 19 – Electronic and Information Warfare This chapter covers topics that have been traditionally more interesting for the military, namely jamming and blocking electronic communications as well as countermeasures and surveillance. In essence the same as in the first edition with a few updates and more explanatory text.

Chapter 20 – Telecom System Security This chapter covers security issues of telephony (such as billing), starting at traditional telephone systems, going on to mobile telephony, and ending at internet telephony. The latter is new compared to the chapter in the first edition; apart from that, a lot of text has been added.

Chapter 21 – Network Attack and Defense This chapter covers quite technical issues (without going too deep into details) of network protocols with respect to security. Topics include, denial of service attacks, spam, various kinds of malware; countermeasures such as filtering and and intrusion detection as well as limitations of those. Compared to the chapter in the first edition, this chapter has seen a major overhaul, especially the section on malware (now including the discussion of rootkits) has been largely revamped; the section on problems in attack detection has been much expanded and covers specific technologies such as WiFi, Bluetooth, IPSec, and others.

Chapter 22 – Copyright and DRM Here the reader finds a discussion of techniques on how to enforce copyright for different media, such as software, audio, video, pay-TV, DVD and Blu-ray, and others, followed by a discussion of rights management systems. The second part of the chapter discusses information hiding strategies and watermarking, as well as policy issues. This chaper is the chapter on protecting e-commerce systems from the first edition.

Chapter 23 – The Bleeding Edge This chapter covers (online) games, web applications such as eBay, google, and social networks, privacy enhancing techniques such as anonymous email, anonymous browsing, and forensics countermeasures, as well as issues of digital elections. This chapter is new.

Chapter 24 – Terror, Justice and Freedom This chapter covers mostly the political and social consequences of terrorism incidents. This chapter is new, although parts of the removed chapter on E-Policy have been moved into this chapter.

Chapter 25 – Managing the Development of Secure Systems This is the largely extended chapter on management issues from the first edition. It covers topics such as risk management, design methodologies, security requirements engineering and team management.

Chapter 26 – System Evaluation and Assurance This chapter deals with the question of what assurance is, how to get it, and how to know that you got it. Anderson discusses issues such as security testing, review, evaluation, as well as Common Criteria and their limitations. This is the updated and largely expanded version of the accordant chapter in the first edition.

2 What is the book like (style)?

Anderson prudently avoids unneccessary technical details, therefore the book is suited for a very broad range of readers. The text is carefully written, always keeping the practitioner in mind. Much emphasis is given to what goes or went wrong and what one can learn from that, and accordingly, you find in almost every chapter sections with according titles. The only shortcoming that I have noted is that Anderson proceeds at times at such a quick pace that it is hard to keep up. Moreover, sometimes he writes statements of which – at least to me – I could not figure out why he wrote them or how they fit into the context (in other words, he makes sometimes very implicit statements – fortunately that happens rather infrequently).

3 Would you recommend this book?

This book, as a whole or the relevant chapters and sections, is morally a must-read for anyone who is involved in the design or implementation of security relevant systems, or who is responsible for the operation or the management of such systems.

The reviewer is a consultant at Secorvo Security Consulting, Karlsruhe, Germany.