
Preface

Authentication and key establishment are fundamental building blocks for securing electronic communications. Cryptographic algorithms for encryption and integrity cannot perform their function unless secure keys have been established and the users know which parties share such keys. It is essential that protocols for providing authentication and key establishment are fit for their purpose.

Although there are certainly earlier publications on techniques for authentication, it is fair to regard the 1978 *Communications of the ACM* paper of Needham and Schroeder as the starting point for the modern study of protocols for authentication and key establishment. There are two main research camps that have advanced understanding of cryptographic protocols since the publication of the Needham–Schroeder paper. These are the *cryptography* community and the *computer security* community. Between them, these communities have produced a vast number of protocols; some would say far too many. This has led to many difficulties for researchers and practitioners who wish to navigate this vast literature. We hope that this book will help them find their way.

We believe that this book is the first comprehensive treatment of protocols for authentication and key establishment. There have, of course, been previous surveys of a more limited nature and these have provided valuable information and examples for us. Particularly useful was the extensive survey of Clark and Jacob [95] which includes a library of some 40 protocols as well as introductory material and an annotated bibliography. Two chapters in the authoritative *Handbook of Applied Cryptography* of Menezes, van Oorschot and Vanstone were also a source of much information. Nevertheless, in virtually all cases we have taken protocol descriptions directly from the original sources.

Our aim has been to provide a comprehensive coverage of our subject matter. Yet, despite restricting ourselves strictly to protocols for authentication and key establishment, we quickly realised that it was unrealistic to be exhaustive. When we started the project in 1999 it seemed to us that there was a certain stability in the field, and this was a strong argument for the time-

liness of the work. To an extent this judgement has turned out to be sound, at least for simple protocols of well-established type. But for more complex protocols we were very definitely wrong, and the problem of trying to draw a definitive picture of an ever changing landscape caused many headaches. This is particularly true of the material on group-oriented protocols and that on password-based protocols. Even as we write this preface, we are aware that new protocols and design techniques are being developed in both these areas.

How to Use This Book

We hope that this book will prove useful both to those who wish to learn more about the field and as a reference for those looking for information about a specific protocol or group of protocols. The first two chapters are introductory and may be useful for the graduate student, or anyone coming to the field for the first time. Material in the remaining five chapters has been arranged thematically to help the reader identify connections between different protocols. Between them, these five chapters survey more than 150 protocols from the literature.

Chapter 1 starts with a tutorial aimed at explaining the general methods of how protocols work and the typical capabilities of protocol adversaries. Definitions for the basic protocol components follow, including a quick overview of cryptographic algorithms and their properties, as well as a list of typical protocol attacks.

Chapter 2 is devoted to a study of the different goals that protocols for authentication and key establishment may have. We believe that this is a critical part of understanding protocol analysis, and neglect of this issue has been the source of much error in the past. The chapter develops a hierarchy of different goals, considering only extensional goals. This hierarchy is used in subsequent chapters to evaluate various protocols. We feel the hierarchy provides a simple yet effective tool for describing protocol properties and for evaluating attacks against protocols with unclear goals. The last section contains a brief survey of formal protocol analysis techniques, broadly divided into those using formal specification and those using complexity-theoretic proofs.

Chapter 3 is concerned with protocols that employ symmetric cryptography. Many of these protocols involve an on-line trusted third party, in the tradition established by Needham and Schroeder.

Chapter 4 deals with protocols using public key cryptography, but excluding key agreement protocols. As in Chap. 2 we include some standardised protocols and also some protocols in wide use today, such as the TLS protocol.

Chapter 5 is concerned with key agreement based on public keys. Most of the protocols in this chapter are based on the Diffie–Hellman key exchange. There is a vast range of protocols in this class, and consequently

this is the longest chapter. There is also a treatment of identity-based key agreement protocols.

Chapter 6 covers conference key protocols. Much of this chapter concerns generalisations of protocols from Chap. 5 to the multi-party setting. In particular, Diffie–Hellman key agreement with multiple parties is discussed in some detail. A topic that is not treated in any depth in this chapter is that of dynamic conferences.

Chapter 7 deals with password-based protocols. Such protocols were first developed not much over 10 years ago. Recently there have been many new protocols proposed in this area, and we have tried to take into account the most important of these.

Appendix A is a brief overview of published standards for authentication and key establishment protocols. Rather than give the details in this appendix, reference is made to many of the standardised protocols described in different chapters of the book.

We expect that the book may be used by the practitioner for tasks such as finding whether an established protocol exists for a specific application, or whether any attacks are known on a specific protocol or on related protocols. To help with such tasks we have provided a list of protocols and a list of attacks in the front matter. There is also an index of protocol names at the back as well as the more usual general index.

We have used a uniform notation for all protocols in the book, and have aimed to present the protocols in a manner that explains the important details clearly, and yet does not give excessive detail. There are different views of how to best achieve this aim, and we have compromised by using two different main presentation techniques. In Chaps. 3 and 4, and occasionally in later chapters, we have used a notation simply showing the messages exchanged between the protocol principals. We have preferred this notation when there are more than two principals involved, and when the interpretation of protocol actions seems straightforward. In most of the protocols in Chaps. 5, 6 and 7 we have used protocol flow diagrams that include principal actions. This notation seems more useful when there are complex and important actions involved. However, these diagrams can get rather cluttered, particularly for conference key protocols.

Acknowledgements

Many people have given their help and advice generously over the several years that it has taken us to produce the book. We would like particularly to acknowledge Paul van Oorschot who looked at an early draft of the book, provided detailed feedback and sterling advice, and also introduced us to Springer. The series editors, Ueli Maurer and Ron Rivest, have also been supportive throughout.

Different people have reviewed and provided comment on various portions of the book. We thank them all for the generous spirit and are sincerely sorry

if we have misinterpreted or forgotten any of their helpful advice. This list includes all those who we can remember; we hope not to have missed anyone.

Ross Anderson	Malcolm Boyd	John Clark
Ed Dawson	Marie Henderson	Yvonne Hitchcock
David Jablon	Yongdae Kim	Philip MacKenzie
Wenbo Mao	Keith Martin	Alfred Menezes
Chris Mitchell	DongGook Park	Josef Pieprzyk
Ron Rivest	Carsten Rudolph	Rei Safavi-Naini
Kapali Viswanathan		

In addition, Daniel Bleichenbacher and Serge Vaudenay provided helpful answers to specific questions we asked of them. We are solely responsible for all errors of fact, presentation style, or just plain typing errors that this book may have.

The team at Springer have been encouraging and helpful throughout. We would particularly like to thank Alfred Hofmann who carefully introduced us to the publication process. Ingeborg Mayer has been an unfailing source of information and advice, and displayed extreme patience as we continually failed to meet our deadlines.

CB would like to record his personal thanks to his family $D + C^3$ who put up with considerable neglect, week after week and month after month, yet remained understanding and supportive. The Information Security Research Centre and the School of Software Engineering and Data Communications at Queensland University of Technology provided time and material support and he would like to acknowledge the encouragement of their respective heads, Ed Dawson and Bill Caelli. He would also like to acknowledge Papa Haydn for sustaining him during many a long working session.

AM would like to thank his wife, Hemal, and daughter, Radhika, for their love and patience throughout this project. His writing of this book was started at the University of Massachusetts at Dartmouth; he would like to acknowledge his colleagues in the Computer and Information Sciences Department at UMASS for their support and encouragement. His current institution, Dhirubhai Ambani Institute of Information and Communication Technology, generously granted him time to complete the book.

This book was typeset in \LaTeX on various different platforms. We used Ron Rivest's `windex` package to help with index preparation. The style for the protocols and attacks is adapted from Anselm Lingau's `float` package.

Brisbane, Gandhinagar
June 2003

Colin Boyd
Anish Mathuria