Review of the book

"Protocols for Authentication and Key Establishement"

by Colin Boyd / Anish Mathuria

Springer, 2003

ISBN: 3-540-43107-1, 978-354-043-1077

Kilian David
Dipl. Wirt.-Informatiker, M.Sc. in Applied IT Security

1 Summary of the review

The book "Protocols for Authentication and Key Establishment" gives an overview about a selection of well-chosen 172 cryptographic protocols. The exceptional work of the authors took four years of reviewing and collecting the original sources for finally presenting them in a comprehensive and appropriate manner. It has a special focus on protocols of well-established type where descriptions of all their related classic attack types (and 36 protocol-specific attack types) are given. More advanced protocols like group-oriented or password-based ones are only handled roughly.

2 Summary of the book

The book is divided in seven chapters which are appropriate for (under-) graduates, post-graduates and professionals as well.

In **chapter 1** an overall introduction to authentication and key establishment is given via describing the different requirements, protocol architectures, cryptographic properties and types of attacks as well as basic design principles. Although the writing style is sometimes colloquial it fits the need of getting started easily and dive more deeper in the topic via describing the "rules of the game". All concepts are first introduced and explained on the basis of creating a hypothetical protocol with lots of common mistakes and their proper handling. Based on this, necessary fundamental concepts of cryptography and methods to ensure freshness are presented. Finally, a survey of attacks on protocols is given, where it is pointed out, that the understanding of protocol failures is essential for designing and assessing unfamiliar protocols. At last, the design principles of Abadi/Needham for cryptographic protocols are given where unfortunately neither an assessment of the quality is given nor any protocol is measured against these requirements.

In **chapter 2** the goals for authentication and key establishment are first defined informally and diversified in basic and enhanced ones. Additional credit is then taken to goals concerning compromised keys but only handled within three pages. The next two subsections are the most interesting ones since their focus is set on formal verification methods and complexity-theoretic proofs of security. With respect to the release date of the book, the authors give a comprehensive overview about different methodologies while referencing the work of related specialists (C. Meadows for example).

The following five chapters are presenting the protocols which are obviously the heart of this book. Every chapter starts with a short introduction of the notations and design principles. The great feature at the end of each chapter is the summary and comparison of the major properties of the protocols presented before. Additional useful information is given about known attacks and the availability of security proofs.

After presenting the protocols using shared key cryptography (**chapter 3**), the protocols for entity authentication and key transport are described which use public key cryptography (**chapter 4**). The fifth

chapter is the longest one and gives a comprehensive overview about key agreement protocols (**chapter 5**). Most of them are based on the well-known Diffie-Hellman key exchange approach and differentiated by the message complexity and their usability on devices with restricted resources like mobile terminal or embedded hardware. This chapter is finished by presenting and explaining protocols which are not based on Diffie-Hellman. At least, **chapter 6** is about conference key protocols and **chapter 7** about password-based protocols. Although the sixth chapter generalizes protocols from chapter five to use them in multi-party settings, the important topic of how to treat dynamic conferences is not handled in this section. Finally, the seventh chapter relies on the interesting assumption that humans are only able to remember passwords with the length of eight characters at maximum. Resulting from this, the presented protocols have been designed to be even secure in situations where the principals share only a password of small entropy.

The appendix covers some frameworks and standards (ISO, IETF, IEEE, NIST and ANSI) where it is possible to comply with or to get certified against.

3 Summary and Recommendation

The book gives a great overview about protocols and their modes of operation. Being suitable for (under-) graduates, post-graduates and even professionals, this reference book can be used to get a quick understanding of the most important protocols. Especially the overview about theoretic and specific attacks gives a useful guidance of what to consider about within the security design.

However, it needs to be mentioned that the use of the protocols presented may be restricted due to the fact of being protected by patent law (the Jason-Tsudik 2PKDP for example is registered under United States Patent 5,729,608). This further information would be a nice (and sophisticated) add-on to complete this comprehensive overview extensively.

In addition to this, the complexity of the different protocols is not mentioned. Although this fact always depends on the kind of implementation, an overview about the state of the art would have been helpful (important technologies are described on a generic level in the paper from Awerbuch et al. "Costsensitive Analysis of Communication Protocols" or for specific two-party communications in the paper from Kushilevitz "Communication Complexity"). Besides the fact, that no hints of implementing the protocols efficiently is given, the book offers a great service for the specific use of theoretic research and gives a comprehensive overview within this area.

The reviewer works as an expert IT-auditor at Volkswagen Financial Services AG, Germany.