Review of the book

"Network-Aware Security for Group Communications"

by Yan Sun, Wade Trappe and K.J.R. Liu

Springer, 2008

ISBN: 978-0-387-68846-6

Reviewer: Choudary Gorantla

1 Summary

This book gives an introduction to group key management protocols in different network settings. It can be recommended to early researchers in the areas of group key management, secure multicast and secure communication in sensor networks. The book discusses various security issues in group communications in a network-aware approach. However, it fails to show how to rigorously analyze group key management protocols with respect to these identified security issues.

The book has 10 chapters. The initial chapters give an overview of generic security issues related to group communications, whilst the later chapters concentrate on specific network/application settings like cellular networks, multimedia multicast and wireless sensor networks etc. Each chapter begins with identifying a research problem and giving an overview of how this is going to be addressed. The contents of each chapter are summarized at the end of the respective chapter.

2 Detailed Description

Chapter 1: This chapter describes the necessity of considering secure group communication. It also gives a brief overview of later chapters.

Chapter 2: This chapter identifies the security requirements of centralized group key management (GKM) protocol. It then presents a basic tree-based GKM protocol that satisfies the identified security requirements. A dynamic version of the basic protocol is also presented. Finally, the efficiency of the protocol is analyzed. This chapter is useful for understanding the basic security requirements of GKM protocols and how to analyze their efficiency.

Chapter 3: This chapter concentrates on group key agreement (GKA) protocols in both homogeneous and heterogeneous networks i.e., networks that contain parties with equal (computational/communication) capabilities and varied capabilities respectively. The authors describe one particular GKA protocol called the "Butterfly" scheme for homogeneous networks and its variant for heterogeneous networks. The efficiency of both the protocols is well analyzed. However, this chapter does not say anything about the security issues that may be specific to GKA protocols. It also chooses to focus on tree-based GKA protocols, ignoring other important GKA protocols in the literature.

Chapter 4: This chapter is about optimizing rekeying costs in dynamic group key agreement protocols. Although the chapter starts with the aim of designing contributory GKE protocols with lowest possible cost, similar to the previous chapter it concentrates only on tree-based contributory GKA protocols. The chapter discusses two contributory GKA schemes which achieve high efficiency among tree-based schemes.

Chapter 5: This chapter discusses a tree based GKM protocol that is suitable for cellular multicasting. A GKM scheme and its dynamic version are presented. Their efficiency is analyzed.

Chapter 6: It gives a good discussion on GKM for specific multimedia applications and also presents some message formats for the protocol messages. The initial parts of the chapter have some information repeated from Chapter 2.

Chapter 7: This chapter concentrates on hierarchical access control that supports multi-level access privilege in group communications. The problem is clearly formulated and the specific security requirements are identified. A centralized multi-group key management scheme is then presented and its efficiency is well analyzed.

Chapter 8: This chapter talks about protecting member information in dynamic GKM protocols. It discusses three types of attacks and then defense techniques to prevent them. The efficiency of the techniques is then analyzed.

Chapter 9: This chapter deals with securing multicast authentication against denial of service attacks. It concentrates on a popular authentication scheme called TESLA. A variant of TESLA that provides multi-grade authentication is then presented. All in all, a good chapter that discusses different types of adversarial scenarios.

Chapter 10: This chapter discusses an authentication framework for hierarchical ad-hoc networks. It is poorly organized and there is no continuity among the sections within the chapter. The framework in this chapter looks interesting but its does not seem to be fully analyzed.

3 Recommendation

Group Key Management is an important concept that forms basis for the security of any group communication. Hence, it is very interesting to see a full book dedicated to group key management in a variety of network/application settings. However, this book does not live up to its title.

The book seems to be a collection of articles previously published by the authors themselves. The chapters are not logically connected and there is some redundancy in many chapters. Chapter 3 and 4, which concentrate on contributory group key agreement protocols, are completely out of place in the middle of centralized group key management techniques. This book spends a lot of pages on elaborated efficiency analyses of different group key management/agreement schemes but cares too little about the security of these schemes.

This book can be recommended to early researchers in the areas of group key management, sensor networks and the application settings discussed in the book. However, this book may only be used as a supplement since it does not provide strong background on any of these areas.

The reviewer is a Ph.D. student at the Information Security Institute, Queensland University of Technology, Australia.