Secure Group Communications over Data Networks

SECURE GROUP COMMUNICATIONS OVER DATA NETWORKS

XUKAI ZOU
Indiana University - Purdue University, Indianapolis
Indianapolis, IN 46202, USA

BYRAV RAMAMURTHY
University of Nebraska-Lincoln
Lincoln, NE 68588, USA

SPYROS S. MAGLIVERAS
Florida Atlantic University
Boca Raton, FL 33431, USA

Springer

Prof. Xukai Zou
Dept. of Computer & Information Science
Purdue University,
School of Science at Indianapolis
723 W. Michigan St. SL280E
Indianapolis, IN 46202 USA
xkzou@cs.iupui.edu

Prof. Byrav Ramamurthy
Dept. of Computer Science & Eng.
University of Nebraska-Lincoln
256 Avery Hall
Lincoln, NE 68588-0115 USA
byrav@cse.unl.edu

Prof. Spyros S. Magliveras
Dept. of Mathematical Sciences
Florida Atlantic University
Boca Raton, FL 33431 USA
spyros@fau.edu

Secure Group Communications Over Data Networks

Library of Congress Cataloging-in-Publication Data

A C.I.P. Catalogue record for this book is available
from the Library of Congress.

ISBN 0-387-22970-1 e-ISBN 0-387-22971-X Printed on acid-free paper.

Printed in the United States of America.

9 8 7 6 5 4 3 2 1 SPIN 11053323

springeronline.com

This book is dedicated to our wives Suqin, Bhuvana, and Leanne.

Contents

List of Figures

List of Tables

Preface

The ubiquitous nature of the Internet is enabling a new generation of applications to support collaborative work among geographically distant users. Security in such an environment is of utmost importance to safeguard the privacy of the communication and to ensure the integrity of the applications.

'Secure group communications' (SGC) refers to a scenario in which a group of participants can receive and send messages to group members, in a way that outsiders are unable to glean any information even when they are able to intercept the messages. SGC is becoming extremely important for researchers and practitioners because many applications that require SGC are now widely used, such as teleconferencing, tele-medicine, real-time information services, distributed interactive simulations, collaborative work, grid computing, and the deployment of VPN (Virtual Private Networks). Even though considerable research accomplishments have been achieved in SGC, few books exist on this very important topic.

The purpose of this book is to provide a comprehensive survey of principles and state-of-the-art techniques for secure group communications over data networks. The book is targeted towards practitioners, researchers and students in the fields of networking, security, and software applications development.

The book consists of 7 chapters, which are listed and described as follows.

Chapter 1. This chapter presents an introductory overview of SGC. The chapter begins by introducing central problems of SGC such as group key management and membership management. It proceeds to introduce secure two party communication techniques and enabling technologies for SGC. Finally, an outline of the subsequent chapters of the book is presented.

Chapter 2. This chapter begins by classifying typical key management protocols based on different criteria such as *public key based* vs. *secret key based*, *centralized* vs. *distributed*, *unconditionally secure* vs. *computationally secure*, and *monolithic* vs. *subgroup-oriented.* Then it explains, in detail, several typical key management protocols including *Naive protocol*, *Secure lock*, *Reversible Parametric Sequence* (RPS), *Secure Transmission Backbone* (STB), *Core Based Tree* (CBT), *Iolus*, *Dual Encryption Protocol* (DEP), and a suite of *n-party Diffie-Hellman* schemes.

Chapter 3. This chapter focuses on a specific family of tree-based key management schemes. Tree-based key management is efficient and scalable, and can be used in one-to-many multicast applications as well as many-to-many group communications. Moreover, it can be centralized as well as distributed. This chapter discusses *Centralized key-tree*, *Centralized One-way Function Tree* (OFT), *Distributed Scalable Secure Communication* (DISEC), *Distributed Tree-based Group Diffie-Hellman key agreement* (TGDH) and *Block-Free Tree based Group Diffie-Hellman key agreement* (BF-TGDH).

Chapter 4. In this chapter, we discuss a specific scenario of SGC, called *dynamic conferencing*, and related key management solutions. By 'dynamic conferencing', we mean that the members of an arbitrary subset of a group are able to form a privileged subgroup and communicate securely within the subgroup. This chapter introduces several schemes such as *naive solution, public key based dynamic conferencing, secure lock based dynamic conferencing, symmetric polynomials based dynamic conferencing*, and *key tree based dynamic conferencing.*

Chapter 5. This chapter presents another specific SGC scenario, namely *SGC with hierarchical access control* (HAC), and related solutions. By 'SGC with HAC', we mean that members in a group are divided into a number of subgroups located at different privileged levels and the members in a higher-level subgroup can receive and decrypt messages from members in any of their descendant lower-level subgroups, but the reverse is not allowed. The following schemes for SGC with HAC are discussed in the chapter: *Akl-Taylor's* scheme, *Lin's* scheme, *Sandhu's* scheme and *Chinese Remainder Theorem based scheme.*

Chapter 6. Apart from group key management, there are other issues which are necessary or helpful for SGC, include *membership management, access control, message/source authentication*, and *non-repudiation.* Chapter 6 addresses some of these topics. Since wireless/mobile networks (and, in particular, ad hoc networks) are becoming increasingly prevalent, SGC will be widely used in wireless environments. However, the specific properties and limitations of wireless/mobile networks pose many new problems in deploying SGC in these environments. The chapter addresses these challenging problems and proposes certain guidelines for solving them.

Chapter 7. This chapter summarizes the topics in the book and concludes by discussing several typical SGC applications including *secure tele-conferencing, secure collaborative work, virtual private networks*, and *secure grid computing.*

As a note to the reader, we wish to mention that we have chosen not to pursue a high degree of integration in the subject matter of this book. Thus, the reader will find different nomenclature, terminology and treatment for similar, or even identical entities, such as, for example, the *Trusted Authority* (TA), versus the *Group Controller* (GC), etc. We have stayed rather close to the original presentation of research papers, seeking integration of material in terms of scope, but without identifying and fusing commonalities. In time, when the SGC subject matter matures, further integration and identification of equivalent notions might be desirable, and even achievable.

We hope you will enjoy reading this book!

XUKAI ZOU, BYRAV RAMAMURTHY, AND SPYROS MAGLIVERAS

Acknowledgments

During the writing of this book we have been helped by many friends and colleagues to whom we are indebted for their comments, criticisms and suggestions. Particular thanks go to Professor Jean-Camille Birget and Professor Guevara Noubir for research collaboration with us in the areas of secure group communications and hierarchical access control. Many thanks are due to all authors whose research results have been included in the book, and to Mr. Alex Greene and Ms. Melissa Sullivan of Kluwer Academic Publishers for their patience and help with the publication of the book. We are indebted to Mr. Ravi Kumar Balachandran who read and edited the manuscript, provided many suggestions, and drew figures. We are grateful to Professor Wandi Wei, Messrs. Daniel Socek and Michal Sramka as well as Ms. Deborah Derrick for reading segments of the text and making useful and significant suggestions. Thanks also to Messrs. Sarang Deshpande, Amandeep Thukral, and Yogesh Karandikar for drawing figures. Finally, our special thanks go to the U.S. National Science Foundation for partial support of this work under grant CCR-0311577.

Chapter 1

INTRODUCTION

"*Secure group communications*" (SGC) refers to a scenario in which a group of participants can send and receive messages to group members, in a way that outsiders are unable to glean any information even when they are able to intercept the messages. Secure group communications rely on the protocols and fast developing theoretical tools of modern cryptology.

1.1 Overview of Secure Group Communications

With the exponential growth in modern communications, SGC is becoming an extremely important research area because of the need to provide privacy and authentication in communications. Many applications that require SGC are now widely used, such as teleconferencing, tele-medicine, real-time information services, distributed interactive simulations, collaborative work, interactive games and the deployment of VPN (Virtual Private Networks).

Because of the importance of SGC, the initial research group SMuG (Secure Multicast Research Group) in IRTF (Internet Research Task Force) for secure multicast has included SGC as its critical research area and a working group, MSEC (Multicast SECurity) in IETF (Internet Engineering Task Force) was established in 2001 to standardize and provide drafts for SGC. Moreover, another research group GSEC (Group SECurity) in IRTF was established in 2001 to investigate problems specific to SGC.

Group communications are implemented using broadcast or multicast mechanisms, such as IP (Internet Protocol) multicast, to provide efficient transmission of group messages. Similar to 'secure two-party communication' (STPC), security of group communication is enforced by cryptographic techniques such as *encryption*, *signatures*, *authentication* and *integrity*. However, because of the intrinsic differences between two-party communications and group communications, techniques, such as key agreement for STPC cannot be directly used for SGC and there are many more problems which need to be solved before SGC can be used in real systems and applications. As a result, even though mature techniques exist for STPC, including many standards and systems, there are currently no standards and available systems for SGC. A few current implementations for SGC such as SecureRing [Kihlstrom et al., 1998], Horus/Ensemble [Rodeh et al., 2001, Rodeh et al., 1998], Rampart [Reiter, 1994], and API's such as CLIQUES [Steiner et al., 1997] and SPREAD (also Secure SPREAD) [Amir et al., 2003] are primarily for research/experimental purpose, and hopefully some of them can be deployed broadly and adapted as standards in the future. There is a considerable number of articles and reports about SGC techniques in the literature. However, there is a dearth of comprehensive books which provide an integrated view of the state-of-the-art in SGC. The objective of this book is to alleviate this problem.

We note that the terms *set* and *group* are synonymous in SGC literature, and so are the terms *subset* and *subgroup*. Thus, *group* and *subgroup* as used here do not have the standard algebraic meaning.

Like in STPC, the secrecy/privacy of group communications is achieved by encrypting group messages with a shared secret, called *group key* in group communication. The group key is only accessible to group members and thus, only group members are able to decrypt the messages. Therefore, the first (and most important) problem facing SGC is *key management*, that is, the methodology that enables group members to establish and distribute shared group keys. A primary feature in SGC is *group dynamics* (also called *member dynamics*). For two-party communications, after the establishment of a communication session, if either party leaves or stops the conversation, the session terminates. However, during a group communication session, members can join or leave the session or group at any time, while the group communication continues. Whenever members join and/or leave the group, the group key needs to be changed in order to guarantee secrecy for the residual, continuing communication group. How to change the key, both efficiently and scalably, is a considerable challenge.

There are some other scenarios related to SGC, which require group key management, such as *dynamic conferencing* and *SGC with hierarchical access control*. 'Dynamic conferencing' refers to a situation where there is a universal group of participants[1] U and any subset S of participants in U is able to form

[1] The terms *participants*, *members*, *users*, and *communicants* are used interchangeably in the book.

a privileged subgroup. We call each possible subgroup S a *conference*. The participants in a conference S are able to communicate in such a way that any participant not in the conference (and consequently anyone outside U) is unable to glean any messages directed to the conference. It is required, moreover, that communications among different conferences will not interfere with one another.

'Secure group communication with hierarchical access control (SGC with HAC)' refers to a scenario where a universal group U of members is divided into a number of subgroups located at different privilege levels so that a high-level subgroup S can receive and decrypt messages directed to S or any of its descendant lower-level subgroups, while lower-level subgroups are not able to decrypt messages directed to parent subgroups. HAC is generally enforced using cryptography based techniques [Birget et al., 2001, Zou et al., 2003] i.e., cryptographic keys play a primary role in access control. Here, members in a higher level subgroup S possess or are able to derive the key of a descendant subgroup T, and consequently are able to access all messages communicated within T. In this volume we discuss typical key management protocols for *dynamic conferencing* and *SGC with hierarchical access control.*

Apart from group key management for SGC, there are some other issues which are necessary or helpful for SGC such as membership management, admission control, message/source authentication (MSA), and non-repudiation. Moreover, SGC in wireless environments is a new application paradigm. We will point out the challenging problems facing all these aspects of SGC and suggest possible solutions in the book.

1.2 Preliminaries

In this section, we present basic concepts and preliminaries used in the rest of the book. These include one-way functions, (one-way) hash function, the Chinese Remainder Theorem (CRT), the Discrete Logarithm Problem (DLP), and symmetric polynomials.

DEFINITION 1.1 *A function $y = f(x)$ is said to be a one-way function if it is easy to compute y from x however it is computationally difficult to compute a preimage x given y.*

DEFINITION 1.2 *A (one-way) function $y = f(x)$ is said to be a (cryptographic) hash function if it is a mapping from a bit-string of arbitrary length to a bit-string of fixed length (i.e., $\{0,1\}^* \rightarrow \{0,1\}^n$) and satisfies the following three properties:*
(1) One-way, that is: given $y \in \{0,1\}^n$, it is difficult find an $x \in \{0,1\}^*$ such that $y = f(x)$.
(2) Matching resistant, that is: given $x \in \{0,1\}^*$, it is difficult to find a $x' \in \{0,1\}^*$ such that $f(x') = f(x)$

(3) Collision resistant, that is, it is difficult to find $x, x' \in \{0,1\}^*$ *such that* $f(x') = f(x)$.

The most important feature of a cryptosystem or secure group communication scheme (SGCS) is its degree of security, i.e. its strength in preventing opponents (attackers) from breaking the system. There are two basic approaches which can be used in discussing the security of a cryptosystem (or an SGCS): *computational security* and *unconditional security.*

DEFINITION 1.3 *A cryptosystem is defined to be computationally secure if the best algorithm for breaking it requires at least N operations, where N is some specified, very large number. On the other hand, a cryptosystem is defined to be unconditionally secure if it cannot be broken by attackers, even if the attackers collude and have infinite computational resources [Stinson, 1995].*

Unconditional security implies that when an opponent does not know the secret key k, then k appears to him as a random element in the key space; that is, the opponent has no way of distinguishing the key k from any other element in the key space. As for computational security, in general, a computationally secure cryptosystem utilizes one-way functions to implement secure communications and other cryptographic protocols. A prominent example is a public-key based system, which is always computationally secure, but never unconditionally secure. On the contrary, secret-key based systems generally belong to the category of unconditional security.

Another approach used to discuss the security of secure group communications (with hierarchical access control), is that of *k-resilient security.*

DEFINITION 1.4 *A scheme (system) is said to have* k-resilient security *if it is secure against the collusion of any subset of up-to k opponents but cannot defend against the collusion of some* $k+1$ *opponents.*

For k-resilient security, the value k is a system security parameter and can be set/selected during the system setup. In general, the larger the k is, the more secure a system will be. In contrast, the system will become more inefficient in terms of both space and time complexity.

There may exist certain scenarios where a group of users are required to decrypt an encrypted message, rather than a single user. A threshold cryptosystem [Desmedt and Frankel, 1989] can be used in such situations. A *(t,n)* threshold scheme does not reveal a secret S unless any t out of n participants, or *shadowholders* work together. Each participant i will have a unique shadow k_i which he/she must keep secret. When any *t-1* shadowholders work together, they cannot receive any information about the secret S. In this way, a secret can be shared by many people. If a share is burned in a fire or someone forgets