Trust and Security in Collaborative Computing

SERIES IN COMPUTER AND NETWORK SECURITY

Series Editors: *Yi Pan (Georgia State Univ., USA) and
Yang Xiao (Univ. of Alabama, USA)*

Published:

Vol. 1: Security in Distributed and Networking Systems
eds. Xiao Yang et al.

Vol. 2: Trust and Security in Collaborative Computing
by Xukai Zou, Yuan-Shun Dai and Yi Pan

COMPUTER AND NETWORK SECURITY

Vol. 2

Trust and Security in Collaborative Computing

Xukai Zou

Indiana University-Purdue University Indianapolis, USA

Yuan-Shun Dai

University of Tennessee, USA

Yi Pan

Georgia State University, USA

World Scientific

NEW JERSEY • LONDON • SINGAPORE • BEIJING • SHANGHAI • HONG KONG • TAIPEI • CHENNAI

Published by

World Scientific Publishing Co. Pte. Ltd.

5 Toh Tuck Link, Singapore 596224

USA office: 27 Warren Street, Suite 401-402, Hackensack, NJ 07601

UK office: 57 Shelton Street, Covent Garden, London WC2H 9HE

British Library Cataloguing-in-Publication Data

A catalogue record for this book is available from the British Library.

TRUST AND SECURITY IN COLLABORATIVE COMPUTING

Computer and Network Security — Vol. 2

Copyright © 2008 by World Scientific Publishing Co. Pte. Ltd.

All rights reserved. This book, or parts thereof, may not be reproduced in any form or by any means, electronic or mechanical, including photocopying, recording or any information storage and retrieval system now known or to be invented, without written permission from the Publisher.

For photocopying of material in this volume, please pay a copying fee through the Copyright Clearance Center, Inc., 222 Rosewood Drive, Danvers, MA 01923, USA. In this case permission to photocopy is not required from the publisher.

ISBN-13 978-981-270-368-2

ISBN-10 981-270-368-3

Printed in Singapore.

This book is dedicated to Xukai's wife Suqin and Yuanshun's wife Jiafeng.
Yi Pan would like to thank Sherry, Marissa and Anna for their love,
support and encouragement during the preparation of the book.

This page intentionally left blank

Preface

Information and communication technologies, along with society's drive for collaboration in the modern world, make "collaborative computing" and its applications possible and even necessary. Trust in such an environment will eventually determine its success and popularity due to people's desire for privacy, integrity and reliability. Today's Internet and existing networks are not trust-oriented in design and might be compromised by many untrustworthy factors, such as hackers, viruses, spam, faults, and system failures. Compared to the two-party interaction model (i.e., the client-server service model), collaborative computing environments are group-oriented, involve a large number of users and shared resources, and are complex, dynamic, distributed, and heterogeneous. These factors offer a good environment for hostile elements to lurk. Besides the previously mentioned untrustworthy factors, collaborative computing environments suffer from dangerous attacks by malicious internal members. Those problems restrain full utilization of the computer systems in collaborative computing. The trusted and secure collaborative computing is one of the objectives for the next generation of the Internet, which is trustworthy and security-oriented. This monograph summarizes the authors' and other researchers' efforts to develop such a trusted environment that possesses high security and reliability for the collaborative computing. The important modules composing the trusted and secure computing environment are elaborated, including Secure Group Communication, Access Control, Dependability, Key Management, Intrusion Detection, and Trace Back. The theories and technologies in this book are illustrated with examples to help readers easily understand. One of the examples in collaborative computing is Grid computing that is popular today. The monograph also discusses security and reliability in grid computing. One typical collaborative computing application is medical

practice and healthcare research based on medical information systems. A real project for developing a nationwide medical information system with high dependability and security is described.

X. Zou, Y. Dai and Y. Pan

Acknowledgments

The authors would like to thank many people for their help during the writing and publishing of the book. We thank the colleagues from World Scientific Inc. for their support and guidance to the book. We also thank the help on editing some content from our students Leah Cardaci, Ashhar Madni and our lead network engineer Scott Orr, on drawing some figures from our students Manish Madhusoodan and Xiang Ran, and on proof-reading from Lori M. Bruns, Associate Faculty in the English Department at IUPUI.

This work was partially supported by the U.S. NSF grant CCR-0311577 and IUPUI RSFG (Research Support Funding Grant).

This page intentionally left blank

Contents

<i>Preface</i>	vii
<i>Acknowledgments</i>	ix
<i>List of Figures</i>	xv
<i>List of Tables</i>	xvii
1. Introduction	1
1.1 Overview of Trusted Collaborative Computing	1
1.2 Basic Concepts in Terms of Security	3
1.3 Basic Concepts in Terms of Reliability	9
1.4 Abbreviations and Notations	13
1.5 Outline	14
2. Secure Group Communication (SGC)	17
2.1 Overview of Secure Group Communication (SGC)	17
2.2 Typical Group Key Management Schemes for SGC	19
2.2.1 Centralized Group Key Distribution	20
2.2.2 De-centralized Group Key Management	26
2.2.3 (Distributed) Contributory Group Key Agreement	29
2.2.4 Distributed Group Key Distribution	32
2.3 Enhanced Group Key Management for SGC	35
2.3.1 SGC for Wireless and Mobile Ad Hoc Networks .	35
2.3.2 Authenticated Key Exchange (AKE)	38
2.3.3 Self-Healing Key Distribution	44
2.3.4 Block-free Group Key Management	48
2.3.5 Secure Dynamic Conferencing	52

2.4	Conclusion	56
3.	Cryptography based Access Control	59
3.1	Overview of Access Control in Collaborative Computing	59
3.2	An Efficient Differential Access Control (DIF-AC) Scheme	64
3.2.1	System Description and Initialization	64
3.2.2	System Dynamics and Maintenance	67
3.2.3	Discussion	68
3.3	Cryptographic Hierarchical Access Control (CHAC) Schemes	71
3.3.1	HAC Model	71
3.3.2	Directly Dependent Key Schemes	73
3.3.3	Indirectly Dependent Key Schemes	75
3.3.4	Polynomial and Interpolation based Schemes	75
3.3.5	An Efficient CHAC Scheme with Locality	77
3.4	A Uniform CHAC Scheme Based on Access Polynomials	79
3.4.1	Principle	80
3.4.2	Key Computation/Derivation	80
3.4.3	Node/Vertex Level Dynamics	81
3.4.4	User Level Dynamics	82
3.4.5	Security and Performance Analysis	83
3.4.6	An Illustrative Example and Experiment Results	87
3.4.7	Discussion	90
3.5	Conclusion	94
4.	Intrusion Detection and Defense	95
4.1	Overview of Intrusion Detection and Defense	95
4.2	Intruding Attacks	96
4.3	Intrusion Detection Models	98
4.3.1	Anomaly Modeling	100
4.3.2	Misuse Modeling	101
4.3.3	Specification Modeling	102
4.4	Intrusion Response	104
4.5	DoS/DDoS Attacks	105
4.5.1	Typical DoS Attacks	105
4.5.2	Distributed Denial of Service (DDoS) Attacks	110
4.6	Typical DoS/DDoS Defense Mechanisms	115
4.6.1	Single-node Defending Method	115

4.6.2	Multiple-node Defending Methods	116
4.6.3	HoneyPot	118
4.7	Defending against DoS/DDoS Attacks–Traceback	119
4.7.1	ICMP Traceback	121
4.7.2	(Probabilistic) IP Packet Marking	122
4.7.3	Hash Based Traceback	123
4.7.4	Hybrid Approach	124
4.7.5	Intrusion Detection and Traceback in Wireless Networks	126
4.7.6	Pushback	127
4.8	Exemplary DoS/DDoS Defense Research Projects and Systems	128
4.8.1	Best Practice Methods	128
4.8.2	D-Ward	130
4.8.3	Netbouncer	130
4.8.4	DefCom	131
4.8.5	SIFF	131
4.8.6	Hop-Count Filtering	132
4.8.7	PacketScore	132
4.8.8	Speak-Up	133
4.9	Secure Overlay Service (SOS)	134
4.10	Conclusion	136
5.	Reliability in Grid Computing	137
5.1	Overview of Reliability in Grid Computing	137
5.2	Grid Service Reliability and Performance	139
5.2.1	Description of the Grid Computing	139
5.2.2	Failure Analysis of Grid Service	141
5.2.3	Grid Service Reliability and Performance	142
5.2.4	Grid Service Time Distribution and Indices	144
5.3	Star Topology Grid Architecture	147
5.3.1	Universal Generating Function	147
5.3.2	Illustrative Example	151
5.4	Tree Topology Grid Architecture	155
5.4.1	Algorithms for Determining the pmf of the Task Execution Time	156
5.4.2	Illustrative Example	159
5.4.3	Parameterization and Monitoring	163
5.5	Conclusion	165

6.	Security in Grid Computing	167
6.1	Overview of Security in Grid Computing	167
6.2	Existing Research on Grid Computing Security	169
6.3	Secure Grid Communication and Controlled Resource Sharing in Grid Computing	173
6.4	Dual-Level Key Management (DLKM)	175
6.4.1	First Level	175
6.4.2	Second Level	177
6.4.3	Combination of Two Levels	177
6.4.4	Security and Algorithm Analysis	178
6.5	Secure Grid Computing by DLKM	184
6.5.1	Access Local Resources	185
6.5.2	Access Remote Resources	186
6.5.3	Data Grid	186
6.5.4	Non-Monitored Grid Service	188
6.5.5	An Illustrative Example	188
6.6	Conclusion	192
7.	Trusted and Seamless Medical Information Systems	193
7.1	Overview of Trusted and Seamless Medical Information Systems	193
7.2	Health Information Technology and Medical Information System	195
7.3	Architecture of the Proposed Secure MIS	197
7.3.1	System Architecture	198
7.3.2	Security Functions Supported by ACP	199
7.3.3	Tele-medicine Service	201
7.3.4	Additional Features Resulting from the ACP Mechanism	202
7.4	Dependable MIS based on Grid Computing Technology .	203
7.5	Conclusion	205
	<i>Bibliography</i>	207
	<i>Index</i>	225

List of Figures

2.1	A typical LKH with an example of a member change (join/leave).	21
2.2	A typical $d - ary$ key tree.	22
2.3	Balanced batch rekeying.	23
2.4	Merging algorithm 1.	23
2.5	Merging algorithm 2.	24
2.6	The Iolus scheme.	27
2.7	Tree based Group Diffie-Hellman key agreement.	30
2.8	A tree showing sponsor for each node.	34
2.9	A new member joins (becomes U_5), U_4 is sponsor and U_3 and U_7 are co-distributors.	34
2.10	Block-Free Tree-based Group Diffie-Hellman key agreement for seamless SGC.	49
2.11	U_0 initiates conference $\{U_0, U_1, U_2, U_3\}$ and k_{0-3} is used as the conference key CK	53
2.12	U_1 initiates conference $\{U_1, U_3, \dots, U_7\}$ and pk_3 and pk_7 are used to encrypt the conference key CK . Then U_7 encrypts CK with k_{4-7}	54
3.1	Binary indexing of keys.	65
3.2	An efficient algorithm for determining the key indices for any RL	66
3.3	Comparing number of shared keys with <i>Navg</i>	69
3.4	A typical hierarchy represented as a DAG.	72
3.5	Assignment of primes, t_i s and keys k_i s.	74
3.6	Independent keys and the corresponding r_{ji} s.	75
3.7	An example of access hierarchy and their key and edge values.	78
3.8	An example	87
3.9	Running times for hiding key: based on number of users.	90

3.10 Running times for hiding key: based on the polynomial degree. 91

3.11 Running times for extracting key: based on number of users. . 92

3.12 Running times for extracting key: based on the polynomial degree. 93

5.1 Grid computing system. 140

5.2 Grid system with star architecture. 148

5.3 Subtask execution precedence constraints for analytical example. 152

5.4 A virtual tree structure of a grid service. 156

6.1 General architecture of grid computing 184

6.2 A part of the sample hierarchy for grid computing. 189

6.3 Performance for generating polynomials to numbers of group
members: (left) running time *vs.* group members (*m*); (right)
time is linear to m^2 190

7.1 ACP based Secure Medical Information System. 199

7.2 A physician and patient access hierarchy. 200

List of Tables

3.1	Complexities of the newly proposed scheme.	87
5.1	Parameters of grid system for analytic example.	151
5.2	Parameters of the MTSTs' paths.	160
5.3	pmf of service time.	163
6.1	Complexities for the first level.	181
6.2	Time complexities for the second level.	182