Protecting Information Sharing in Distributed Collaborative Environment

PH.D DISSERTATION

BY

LI, MIN

A DISSERTATION SUBMITTED TO THE UNIVERSITY OF SOUTHERN QUEENSLAND IN FULLFILLMENT OF THE REQUIREMENTS FOR THE DEGREE OF DOCTOR OF PHILOSOPHY

COMPUTER SCIENCE

PRINCIPAL SUPERVISOR: DR. HUA WANG
ASSOCIATE SUPERVISOR: DR. ASHLEY PLANK

SEPTEMBER, 2010
DEDICATION

Dedicated to my parents Zicheng Li and Xinhua Jian
and
my husband Xiaoxun Sun
STATEMENT

I hereby declare that the work presented in this dissertation is in my own and is, to the best of my knowledge and belief, original except as acknowledgement in the text. It has not previously been submitted either in whole or in part for a degree at this or any other university.

Min Li

Signature of Candidate Date

ENDORSEMENT

Signature of Supervisor Date
ACKNOWLEDGEMENT

Research is never conducted in isolation. Rather, numerous people have contributed to this thesis through their ideas, discussions, feedback, and support.

First and foremost, I would like to thank my advisor Dr. Hua Wang. His guidance and insight have shaped me as a researcher, and I am extremely fortunate to have had the opportunity to work with him over the past few years. In addition, I would like to thank Dr. Ashley Plank for his support, feedback, and encouragement.

I also owe a great deal of gratitude to the Centre for Systems Biology (CSBi), Department of Mathematics & Computing, Faculty of Science and Research and Higher Degree office of University of Southern Queensland for providing the excellent study environment and financial support. It is a great pleasure to study at the Department of Mathematics & Computing. I also acknowledge Mr. Greg Otto for his help on proof-reading the dissertation.

Finally, on a personal note, I would never have made it this far without the continued support and encouragement of my family: Zicheng Li, Xinhua Jian, Gang Li, and Xiaoxun Sun.
This thesis focuses on three aspects (i.e., role-based access control, role-based delegation and privacy-aware access control) of developing a systematic methodology for information sharing in distributed collaborative environments. We develop techniques for setting up secure group communication and providing accesses to group members for many database systems, which incorporate new security constrains and policies raised by current information technologies. We create new forms of access control models to identify and address issues of sharing information in collaborative environments and to specify and enforce privacy protection rules to support identified issues.

In role based access control systems (RBAC) permissions are associated with roles, and users are made members of appropriate roles thereby acquiring the roles’ permissions. This greatly simplifies management of permissions. Roles are created for various job functions in an organization and users are assigned roles based on their responsibilities and qualifications. Users can be easily reassigned from one role to another. Roles can be granted new permissions as new applications and systems are incorporated, and permissions can be revoked from roles as needed. The principal motivation of RBAC is to simplify administration. In large organizations the number of roles can be in the hundreds or thousands, and users can be in the tens or hundreds of thousands, maybe even millions. Effective management of permission-role assignment could be very useful in practice to avoid the security breach, especially when conflicting permissions granted to the same role. Constraints are an important aspect of RBAC and are a powerful mechanism for laying out higher level organizational policy. Even for the usage control (UCON) model, constraints are discussed less and no formal language is proposed to describe constraints precisely. An appealing is to study constraints formally in RBAC and UCON models. Our work looks at proposing formal approaches to
check conflicts and help allocate permissions without compromising security in RBAC and proposing a formal language to specify constraints for system designers and administrators in UCON models.

Delegation requirement arises when a user needs to act on another’s behalf to access resources. Essentially, in a multi-agent system, delegation becomes the primary mechanism of inter-agent collaboration and cooperation. However, the previous delegation model could not work efficiently in large systems and perform the sensitive delegation task within the broad area of security. In this thesis, we introduce a flexible ability-based delegation model within RBAC. Moreover, to avoid risk during the delegation process, we propose a secure multi-level delegation model, where a projection between the reliability of delegatees and the sensitivity of delegated tasks is built. Our multi-level delegation model allows that a delegatee in a higher trust level can be assigned with a higher level task.

With the widespread use of information technology, privacy protection becomes a major concern and it could not be easily achieved by traditional access control models. In this thesis, we propose a privacy-aware access control model with generalization boundaries, which could maximize data usability while, minimizing disclosure of privacy. Moreover, our privacy-aware access control model provides a much finer level of control. Although Hippocratic database enforced the fine-grained disclosure policy through creating a privacy authorization table, but it does not allow to distinguish which particular method is used for fulfilling a service in a real world case. We use a goal-oriented approach to analyze privacy policies of the enterprises involved in a business process, in which one can determine the minimum disclosure of data for fulfilling the root purpose with respect to customer’s maximum trust. We provide efficient algorithms to automatically derive the optimal way of authorizations needed to achieve a service from enterprise privacy policies.
# Table of Contents

1 Introduction  
   1.1 Problem Statement 21  
   1.2 Methodology 23  
   1.3 Contributions 25  
   1.4 Organization of the Thesis 26  

2 Advanced Permission-Role Relationship in RBAC 28  
   2.1 Introduction 28  
   2.2 Motivation and problem definitions 31  
   2.3 Authorization granting and revocation algorithms 34  
   2.4 Applying the relational algebra algorithms 38  
      2.4.1 The anonymity scalable electronic payment scheme 39  
      2.4.2 Applying the authorization granting algorithm 41  
      2.4.3 Application of the authorization revocation algorithm 42  
   2.5 Related work and comparisons 45  
   2.6 Summary 45  

3 ABDM: An Extended Flexible Delegation Model in RBAC 46  
   3.1 Introduction 46  
   3.2 Ability, group and authorization assignment 48  
   3.3 Ability-based delegation model (ABDM) 50  
      3.3.1 Ability-based user-user delegation 51  
      3.3.2 Ability-based User-Group delegation 53  
      3.3.3 Ability-based delegation authorization 56
3.4 Related work and comparisons ........................................... 58
3.5 Summary ..................................................................... 59

4 MULTI-LEVEL DELEGATIONS WITH TRUST MANAGEMENT 60
4.1 Introduction .................................................................. 60
4.2 Motivation ................................................................... 62
4.3 Trust evaluation ............................................................. 64
4.4 The multi-level delegation model ..................................... 68
   4.4.1 The delegation model ................................................. 69
   4.4.2 Types of delegations ................................................ 72
4.5 Experimental evaluations ................................................. 73
4.6 Related work .................................................................. 77
4.7 Summary ..................................................................... 78

5 SPECIFYING USAGE CONTROL MODEL WITH OBJECT CONSTRAINT LANGUAGE 79
5.1 Introduction ................................................................. 79
5.2 Motivation and related technologies ................................. 81
   5.2.1 Usage control ........................................................... 81
   5.2.2 Unified modeling language and object constraints language .. 83
5.3 Constraints in UCON ..................................................... 84
5.4 Specifying usage control model with OCL ......................... 86
   5.4.1 $UCON_{preA}$ – pre-authorization models ...................... 86
   5.4.2 $UCON_{onA}$ – ongoing-authorization models .................. 88
   5.4.3 $UCON_{preB}$ – pre-obligations models ......................... 90
   5.4.4 $UCON_{onB}$ – ongoing-obligations models .................... 92
   5.4.5 $UCON_{preC}$ – pre-conditions model ............................ 93

TABLE OF CONTENTS
5.4.6 UCON onC – ongoing-conditions model ........................................ 94
5.5 Related work .................................................................................. 94
5.6 Summary ......................................................................................... 96

6 PRIVACY-AWARE ACCESS CONTROL WITH GENERALIZATION BOUNDARIES 97
6.1 Introduction ..................................................................................... 97
6.2 Motivation ....................................................................................... 100
6.3 Privacy-aware access control model .................................................. 103
   6.3.1 Generalization boundary ........................................................... 103
   6.3.2 Privacy-aware authorizations .................................................... 105
   6.3.3 Authorization Specification ...................................................... 107
6.4 Access control process ..................................................................... 109
   6.4.1 Trust-based decision mechanism ................................................. 110
   6.4.2 Ongoing access control mechanism ............................................. 114
6.5 State transitions ............................................................................. 116
6.6 Experimental evaluations ................................................................. 120
6.7 Related work ................................................................................... 125
6.8 Summary ......................................................................................... 127

7 OPTIMAL PRIVACY-AWARE PATH IN HIPPOCRATIC DATABASES 128
7.1 Introduction ..................................................................................... 128
7.2 Motivation ....................................................................................... 131
7.3 Overview of Hippocratic databases .................................................... 133
7.4 Purpose directed graph with delegation ............................................. 134
7.5 Finding Optimal Privacy-aware Path ............................................... 137
   7.5.1 Objective characterization ......................................................... 137

TABLE OF CONTENTS
<table>
<thead>
<tr>
<th>Chapter</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.5.2</td>
<td>The algorithm</td>
<td>139</td>
</tr>
<tr>
<td>7.6</td>
<td>Related work</td>
<td>145</td>
</tr>
<tr>
<td>7.7</td>
<td>Summary</td>
<td>148</td>
</tr>
<tr>
<td>8</td>
<td>CONCLUSION</td>
<td>149</td>
</tr>
<tr>
<td>8.1</td>
<td>Conclusion</td>
<td>149</td>
</tr>
<tr>
<td>8.2</td>
<td>Future work</td>
<td>151</td>
</tr>
</tbody>
</table>
# List of Figures

2.1 RBAC relationship ........................................... 30  
2.2 Administrative role and role relationships in a bank ........ 31  
2.3 Local revocation ........................................... 38  
2.4 Global revocation ........................................... 38  
2.5 Electronic cash model ....................................... 41  
2.9 ROLE-PERM relation ....................................... 41  
2.6 User-role assignment in the payment scheme ................. 42  
2.7 Administrative role assignment in the scheme ............... 43  
3.1 Example of ability delegation ................................ 51  
3.2 Role hierarchy in *POS* ................................... 57  
3.3 Example of Group Delegation ................................ 57  
4.1 Weighted least-squares exponential regression ............... 65  
4.2 Distribution of delegations based on trust levels .......... 69  
4.3 (a) The precision of the trust value; (b) The precision of the trust trend. . . 75  
4.4 Disclosure rate comparison .................................. 76  
5.1 Components of UCON model ................................ 82  
5.2 Continuity and mutability properties of UCON .............. 83  
6.1 Authorization tree .......................................... 108  
6.2 Trust evaluation ........................................... 111  
6.3 The state transition of privacy-aware access control model . 118  
6.4 Time and space complexity varying data percentage ........ 121
6.5 Time and space complexity varying the number of attributes . . . . . . . . 122
6.6 Time and space complexity varying the number of generalization levels . . 123
6.7 Disclosure rate comparison . . . . . . . . . . . . . . . . . . . . . . . . . 124
7.1 Purpose directed graph . . . . . . . . . . . . . . . . . . . . . . . . . . . . 136
7.2 $sub_{PDG}$ in Purpose directed graph . . . . . . . . . . . . . . . . . . . . . 142
7.3 Optimal privacy-aware path . . . . . . . . . . . . . . . . . . . . . . . . . . 146

LIST OF FIGURES
# List of Tables

2.1 Example of the relation PERM ........................................... 33
2.2 SEN-JUN relation in Figure 2.2 ....................................... 34
2.3 Example of relation ROLE-PERM .................................... 34
2.4 Example of *can-assignp-M* in Figure 2.2 .......................... 34
2.5 Example of *can-assignp-IM* in Figure 2.2 ......................... 34
2.6 *can-revokep-M* in Figure 2.2 ........................................ 35
2.7 *can-revokep-IM* in Figure 2.2 ...................................... 35
2.10 *Can-assignp-M* of Figure 2.6 ...................................... 43
2.11 *Can-revokep-M* ......................................................... 44
3.1 Example of *can_delegatea* ............................................ 55
3.2 Example of *del_revokea* ................................................ 55
4.1 The classification of delegation tasks ................................. 62
4.2 Distributions of the data sets .......................................... 73
6.1 Privacy information and Metadata .................................... 101
6.2 Private information for *Delivery* purpose ......................... 101
6.3 Generalization boundaries for *Delivery* purpose .................. 104
6.4 Ideal information for *Delivery* purpose .............................. 104
6.5 Example of trust calculation for data user *u* ....................... 112
6.6 Summary of attributes .................................................. 121
7.1 Database schema .......................................................... 134
7.2 Privacy metadata schema ................................................. 134
7.3 Albert’s personal preferences ............................................. 145