Copyright is owned by the Author of the thesis. Permission is given for a copy to be downloaded by an individual for the purpose of research and private study only. The thesis may not be reproduced elsewhere without the permission of the Author.
A Model of Distributed Rights Allocation in Online Social Interaction

A thesis presented in partial fulfillment of the requirements for the degree of

Doctor of Philosophy

in

Information Technology

at

Massey University,
Albany, Auckland, New Zealand

Adnan Ahmad

2013

This research was sponsored by the National Science Foundation (NSF), U.S. under contract no. 0968445. However, the views and conclusions contained in this dissertation are those of the author and should not be interpreted as representing the official policies, either expressed or implied, of NSF, or of the U.S. government or any other entity.
Abstract

In computing, the management of information resources is done through access control, a process by which authorized users are granted permission over resources. The last decade has witnessed the emergence of socio-technical systems (STS) like Facebook, Twitter, and YouTube, where millions of users interact with each other and share billions of resources on a daily basis. Access control for a STS is different from traditional systems in having to satisfy the social requirements of the community as well as the technical requirements of the system.

The problems traditional access control models face today are firstly the complexity of mapping millions of users to billions of resources, and secondly the social requirements of users who want to own the resources they post. Current access control models for STS manage access through rule semantics, roles, trust, history management or contents. However, there is no general logical scheme that allows users to allocate rights, covering not just transfer and delegation but also joint and several ownership.

The trend from centralized to distributed access control demands a general model to manage rights allocation for users having heterogeneous privacy policies. The model's validity derives from socio-technical design, where social requirements like ownership, freedom and privacy give technical access axioms. The aim is to satisfy not only technical but also social requirements, over which the success of today’s software depends.

This research first proposes the social access control model for supporting local administration, dynamic asymmetric relationships and object privacy classification. This core model is then used as a basis of various rights allocation models. The research further illustrates a rights allocation framework based on various properties of STS and presents a reduction approach to design the model. This framework reduces all the possible rights allocations into four basic models: Replace, Revoke, Share and Merge, which can manage every tweet, every post, and every single communication on any STS. The proposed rights allocation models are demonstrated on various current and hypothetical use-cases of current STS to show that it can be used in any system that has social interactions, and where users want to control their resources. This research extends the online social interactions in STS to new horizons which are currently restricted due to the limitations posed by current technology.
Acknowledgement

My success(es) are not through my individual effort alone, but rather through the combined efforts of many.

~Maori proverb

First and foremost, I would like to praise and thank Allah Almighty for bestowing upon me the wisdom, courage, patience and blessings to complete such a huge research endeavor. Thanks Allah, You have given me the power to believe in my passion and pursue my dreams. I could never have done this without the faith I have in you.

The most important person I would like to thank is Dr. Brian, my supervisor, for his support and care during this long and tiring journey. As a “mathematician is a machine for converting coffee into theorems”, Dr. Brian is a mind for converting complex, detailed theorems into amazingly simple ‘two-liners’. Whenever I struck in some problem, he always had a cheerful smile with a mind boggling direction, and a friendly suggestion to enjoy the beautiful weather and God's other blessings bestowed upon us. I have learned a lot from him in terms of research and leading a joyful life – to disconnect from the ‘connected’ world. He really taught me to appreciate the beauty of life along with my goals. Dr. Brian, I will surely miss our long thoughtful discussions. I wish I could stay with you a little longer as I still have to learn a lot from you.

I take immense pleasure in thanking Dr. Lech, my co-supervisor, for his friendly attitude that he has maintained towards me throughout these years. I found a thoughtful supervisor, a caring elder and a cherish friend in his form. His concern for his every single student, cycle stealing from his busy schedule to adjust one of us was quite impressive. Dr. Lech, you are more than a supervisor to me and for that I am really thankful to you. I wish, I can carry on our relation in the future, and it may get stronger with time.

I would like to thank Dr. Yasir and Dr. Sohaib for their support throughout these years. Their room was the ‘chamber of secrets’ for our lively discussions, absurd ideas and what not! I especially thank Dr. Sohaib for reading out this dissertation and helping to improve its presentation.
Also, I wish to express my sincere gratitude to Dr. Tony Norris, Dr. David Parsons, Dr. Andre Barczak, Dr. Andrew Colarik, Dr. Daniel Playne and Mrs. Siew Whitworth for their valuable suggestions. I am also obliged to many anonymous conference and journal reviewers who helped to improve the quality of my papers and thus this dissertation quite substantially.

Finally, I am forever indebted to my parents. I can barely find words to express their endless love, unconditional support and encouragement when it was most needed. Mama and Papa, I cannot thank you enough for being there. If it was not for you I cannot accomplish my greatly desired dream!
# Table of Contents

## CHAPTER 1: INTRODUCTION ....................................................................................... 1  
1.1 PROBLEM STATEMENT .......................................................................................... 3  
   1.1.1 Complexity...................................................................................................... 4  
   1.1.2 Privacy...........................................................................................................  4  
   1.1.3 Operations.....................................................................................................  5  
   1.1.4 Local ownership............................................................................................  5  
1.2 RESEARCH OBJECTIVES AND SCOPE................................................................... 6  
1.3 GUIDE TO THIS DISSERTATION.............................................................................. 7

## CHAPTER 2: STATE OF THE ART ............................................................................... 10  
2.1 THE ORIGIN OF ACCESS CONTROL................................................................. 11  
2.2 POLICIES, MECHANISMS AND MODELS......................................................... 11  
   2.2.1 Access control policies.................................................................................. 12  
   2.2.2 Access control mechanism .......................................................................... 12  
   2.2.3 Access control model.................................................................................... 12  
2.3 THE EVOLUTION OF ACCESS CONTROL.......................................................... 13  
   2.3.1 Bell-LaPadula model.................................................................................... 13  
   2.3.2 Biba’s integrity model.................................................................................... 13  
   2.3.3 DoD models.................................................................................................. 14  
   2.3.4 Clark Wilson model...................................................................................... 14  
   2.3.5 Chinese wall policy...................................................................................... 15  
   2.3.6 Role based access control.......................................................................... 15  
   2.3.7 Rule based access control.......................................................................... 16  
   2.3.8 Distributed environments.......................................................................... 16  
   2.3.9 Customized access control models............................................................. 16  
2.4 SOCIO-TECHNICAL SYSTEMS...................................................................... 17  
   2.4.1 Socio-technical design............................................................................... 20  
2.5 TYPES OF STS......................................................................................... 21  
   2.5.1 One-to-one................................................................................................. 22
3.1.3 Privacy..................................................................................................................59
3.1.4 Relationships...........................................................................................................59
3.1.5 Objects’ local visibility............................................................................................60
3.1.6 Object classification...................................................................................................62
3.2 ACCESS CONTROL SPECIFICATIONS................................................................................62
  3.2.1 Actors..................................................................................................................63
  3.2.2 Objects..................................................................................................................64
    3.2.2.1 Items..................................................................................................................64
    3.2.2.2 Spaces.............................................................................................................64
  3.2.3 Operations...............................................................................................................65
  3.2.4 Rights...................................................................................................................65
    3.2.4.1 Meta-Rights......................................................................................................67
  3.2.5 Authorization authority............................................................................................67
    3.2.5.1 Central administration......................................................................................68
    3.2.5.2 Ownership administration...............................................................................68
  3.2.6 Operations on rights...................................................................................................69
    3.2.6.1 Rights allocation...............................................................................................70
      3.2.6.1.1 Replace.......................................................................................................71
      3.2.6.1.2 Share..........................................................................................................71
      3.2.6.1.3 Merge.........................................................................................................71
      3.2.6.1.4 Revoke.......................................................................................................71
  3.3 CHARACTERISTICS OF RIGHTS ALLOCATION ................................................................72
  3.3.1 Consent..................................................................................................................72
  3.3.2 Totality.................................................................................................................72
  3.3.3 Cardinality.............................................................................................................73
  3.3.4 Monotonicity.........................................................................................................73
  3.3.5 Depth...................................................................................................................74
  3.3.6 Revocation............................................................................................................74
  3.4 REDUCTION APPROACH............................................................................................75
  3.4.1 Mutual exclusive allocation......................................................................................75
    3.4.1.1 Cardinality.......................................................................................................75
    3.4.1.2 Totality.............................................................................................................76
    3.4.1.3 Consent............................................................................................................77
CHAPTER 4: SOCIAL ACCESS CONTROL MODEL

4.1 OWNERSHIP FRAMEWORK

4.1.1 Role assignment

4.1.1.1 Owner

4.1.1.2 Parent

4.1.1.3. Offspring

4.1.1.4. General public

4.1.2 Space initial configuration

4.2 YOUTUBE CREATE PROCESS DEMONSTRATION

4.3 SOCIAL ACCESS CONTROL MODEL

4.3.1 Definitions

4.3.2 Components

4.3.2.1 Namespace

4.3.2.2 Local roles

4.3.2.3 Object classes

4.3.2.4 Attestation certificates

4.3.3 System architecture

4.3.4 Definition

4.3.5 The access control process

4.3.6 Theoretical assessment

4.4 IMPROVEMENTS OVER PREVIOUS MODELS

4.5 SUMMARY
CHAPTER 5: USE-RIGHTS MODEL

5.1 REPLACE USE MODEL

5.1.1 Characteristics of Replace USE

5.1.1.1 Consent

5.1.1.2 Totality

5.1.1.3 Cardinality

5.1.1.4 Monotonicity

5.1.1.5 Depth

5.1.2 Replace USE process

5.1.3 Definition

5.1.4 Rights analysis

5.1.5 Design principles

5.1.6 Revocation

5.1.6.1 Self revocation

5.1.6.2 Time based revocation

5.1.6.3 Rule based revocation

5.1.6.4 The Replace USE revoke process

5.1.7 Summary of Replace USE

5.2 SHARE USE MODEL

5.2.1 Characteristics of Share USE

5.2.1.1 Consent

5.2.1.2 Totality

5.2.1.3 Cardinality

5.2.1.4 Monotonicity

5.2.1.5 Depth

5.2.2 Share USE process

5.2.3 Definition

5.2.4 Rights analysis

5.2.5 Design principles

5.2.6 Revocation

5.2.6.1 Self revocation

5.2.6.2 Time based revocation

5.2.6.3 Rule based revocation
5.2.6.4 The Share Use revoke process ................................................................. 122
5.2.7 Summary of Share Use .............................................................................. 123

5.3 MERGE USE MODEL ..................................................................................... 123
5.3.1 Characteristics of Merge Use ...................................................................... 125
  5.3.1.1 Consent ..................................................................................................... 126
  5.3.1.2 Totality ..................................................................................................... 126
  5.3.1.3 Cardinality ............................................................................................... 127
  5.3.1.4 Monotonicity ........................................................................................... 128
  5.3.1.5 Depth ....................................................................................................... 129

5.3.2 Merge Use process ..................................................................................... 129
5.3.3 Definition .................................................................................................... 130
5.3.4 Rights analysis ............................................................................................. 131
5.3.5 Design principles ......................................................................................... 133
5.3.6 Revocation ................................................................................................... 134
  5.3.6.1 Self revocation ......................................................................................... 134
  5.3.6.2 Time based revocation ............................................................................ 135
  5.3.6.3 The Merge Use revoke process ............................................................... 135

5.3.7 Summary of Merge Use .............................................................................. 135
5.4 CHAPTER SUMMARY ..................................................................................... 136

CHAPTER 6: META-RIGHTS MODEL ................................................................ 137

6.1 REPLACE META MODEL ............................................................................... 138
6.1.1 Characteristics of Replace Meta ................................................................. 139
  6.1.1.1 Consent .................................................................................................. 140
  6.1.1.2 Totality .................................................................................................. 141
  6.1.1.3 Cardinality ............................................................................................. 142
  6.1.1.4 Monotonicity ........................................................................................ 142
  6.1.1.5 Depth .................................................................................................... 143

6.1.2 Replace Meta process ............................................................................... 144
6.1.3 Definition ................................................................................................... 145
6.1.4 Rights analysis ............................................................................................. 145
6.1.5 Design principles ......................................................................................... 148
CHAPTER 7: ANALYSIS ................................................................................................. 174

7.1 MODEL PERMUTATIONS AND THEIR PRECEDENCE ......................................................... 174

7.1.1 Use-Rights permutations ........................................................................................... 175

7.1.1.1 Observations ........................................................................................................ 176

7.1.2 Meta-Rights permutations ...................................................................................... 178

7.1.2.1 Observations ........................................................................................................ 178

7.2 SIMILARITIES BETWEEN USE-RIGHTS AND META-RIGHTS MODELS ............................... 179

7.2.1 Replace model ......................................................................................................... 180

7.2.1.1 Similarity analysis ............................................................................................... 180

7.2.1.2 Precedence analysis ........................................................................................... 184

7.2.1.3 Order analysis ................................................................................................... 185

7.2.2 Share model .......................................................................................................... 185

7.2.2.1 Similarity analysis ............................................................................................... 185

7.2.2.2 Precedence analysis ........................................................................................... 189

7.2.2.3 Order analysis ................................................................................................... 190

7.2.3 Merge model .......................................................................................................... 190

7.2.3.1 Similarity analysis ............................................................................................... 190

7.2.3.2 Precedence analysis ........................................................................................... 194

7.2.3.3 Order analysis ................................................................................................... 195

7.3 COMPLETENESS .......................................................................................................... 195

7.4 SUMMARY .................................................................................................................... 197

CHAPTER 8: DEMONSTRATION ............................................................................... 198

8.1 BASIC USE-CASES ......................................................................................................... 199

8.1.1 Creation use-case ...................................................................................................... 199

8.1.1.1 Facebook ............................................................................................................. 199

8.1.1.2 Orkut ................................................................................................................... 199

8.1.1.3 YouTube ............................................................................................................. 199

8.1.1.4 Wikipedia ............................................................................................................ 200

8.1.1.5 Knowledge management systems ......................................................................... 200

8.1.1.6 Discussion ........................................................................................................... 200

8.1.2 System administrator rights .................................................................................... 200
8.1.2.1 Facebook ......................................................................................................................... 200
8.1.2.2 Orkut ................................................................................................................................... 201
8.1.2.3 YouTube ............................................................................................................................ 201
8.1.2.4 Wikipedia ............................................................................................................................ 201
8.1.2.5 Knowledge management system ......................................................................................... 201
8.1.2.6 Discussion ........................................................................................................................... 202

8.1.3 General public rights ............................................................................................................ 202
8.1.3.1 Facebook ............................................................................................................................ 202
8.1.3.2 Orkut ................................................................................................................................... 202
8.1.3.3 YouTube ............................................................................................................................ 202
8.1.3.4 Wikipedia ............................................................................................................................ 203
8.1.3.5 Knowledge management system ......................................................................................... 203
8.1.3.6 Discussion ........................................................................................................................... 203

8.1.4 Contents creation .................................................................................................................. 203
8.1.4.1 Facebook ............................................................................................................................ 203
8.1.4.2 Orkut ................................................................................................................................... 204
8.1.4.3 YouTube ............................................................................................................................ 204
8.1.4.4 Wikipedia ............................................................................................................................ 204
8.1.4.5 Knowledge management system ......................................................................................... 205
8.1.4.6 Discussion ........................................................................................................................... 205

8.2 ADVANCE USE-CASES ............................................................................................................. 205
8.2.1 Facebook ............................................................................................................................... 205
8.2.1.1 Friends Rights Management ............................................................................................... 206
8.2.1.2 Tagging a photo ................................................................................................................... 206
8.2.1.3 Sharing a video ................................................................................................................... 206
8.2.1.4 Persona sharing .................................................................................................................. 207
8.2.1.5 Persona merge .................................................................................................................... 207
8.2.1.6 Persona rights delegation ................................................................................................... 208
8.2.1.7 Persona transfer ................................................................................................................ 208

8.2.2 YouTube ............................................................................................................................... 208
8.2.2.1 Video transfer ..................................................................................................................... 208

8.2.3 Wikipedia ............................................................................................................................... 209

8.2.4 Knowledge management system .......................................................................................... 209
8.2.4.1 Track delegation .................................................................................................................. 209
List of Figures

Figure 1.1: Guide to this dissertation .................................................................................................................. 9
Figure 2.1: Socio-technical system levels and requirements (Source: Whitworth, 2009, page 5) ....................... 19
Figure 2.2: Summary of the literature and contribution of the current research ........................................ 47
Figure 2.3: The general methodology used in this research (adopted from Kasanen et al., 1993) ............... 51
Figure 2.4: Detailed illustration of the innovation phase using incremental Extreme Formal Modeling (XFM) .... 55
Figure 3.1: A simple social network .................................................................................................................. 57
Figure 3.2: Access control matrix magnitude for different models based on eq. [3.1] and eq. [3.4] for Facebook statistics .......................................................................................................................... 62
Figure 3.3: Reduction approach illustrated as a tree structure outlining various rights allocation models for online social interactions ........................................................................................................ 76
Figure 4.1: Distributed access control model system architecture ................................................................... 89
Figure 4.2: Access control matrix magnitude for different models based on [eq. 3.4] and [eq. 4.11] .......... 93
Figure 5.1: Replace use scenario depicting a running conference ................................................................. 99
Figure 5.2: Sharing use-rights scenario depicting a VOD system ................................................................. 113
Figure 5.3: Merge use-rights scenario depicting collaborative software .................................................... 125
Figure 6.1: Transfer scenario depicting copyright of accepted paper ......................................................... 140
Figure 6.2: Sharing meta-rights scenario depicting Facebook wall ............................................................. 152
Figure 6.3: Meta-rights merge scenario depicting an Internet forum ......................................................... 164
Figure 7.1: Visual description of formation of use-rights allocation permutation table ............................... 177
List of Tables

Table 2.1: Evolution of access control models based on application requirements ................................................................. 17
Table 2.2: Type of STS and their respective online social interactions types ............................................................................. 23
Table 2.3: Various operations on rights and their definitions ........................................................................................................ 36
Table 3.1: Rights Allocation for use-rights and meta-rights ........................................................................................................ 71
Table 4.1: Right for different roles associated with the created object .......................................................................................... 83
Table 4.2: Abbreviations and their definitions ................................................................................................................................. 86
Table 5.1: Delegator and delegatee rights over different objects before and after delegation .................................................. 106
Table 5.2: Rights for different roles associated with the object before and after delegation ......................................................... 107
Table 5.3: Difference between proposed and traditional delegation models .......................................................................................... 111
Table 5.4: Owner and beneficiary rights over different objects before and after the Share Use model ........................................ 119
Table 5.5: Rights for different roles associated with object before and after the Share Use model ............................................... 120
Table 5.6: Owner and beneficiary rights over different objects before and after the Merge Use model ...................................... 132
Table 5.7: Rights for different roles associated with the object before and after the Merge Use model ...................................... 132
Table 6.1 (a): Rights for different old roles associated with object before and after the Replace Meta model ......................... 146
Table 6.1 (b): Rights for different new roles associated with object before and after the Replace Meta model ......................... 147
Table 6.2: Old and new owner rights over different objects before and after the Replace Meta model ........................................ 147
Table 6.3: Difference between proposed and traditional delegation models .......................................................................................... 149
Table 6.4: Rights for different roles associated with the object before and after the Share Meta model .......................................... 158
Table 6.5: Primary and Secondary Owner rights over different objects before and after the Share Meta model ......................... 159
Table 6.6: Rights for different roles associated with object before and after the Merge Meta model ............................................ 170
Table 6.7: Primary and Joint Owner rights over different objects before and after the Merge Meta model ................................. 170
Table 7.2: Precedence of various use-rights model applications over each other ................................................................. 178
Table 7.4: Precedence of various meta-rights model applications over each other ................................................................. 179
Table 7.5: Output summary of Replace Use and Replace Meta models .............................................................................................. 180
Table 7.6: Comparison of various characteristics of Replace model ................................................................................................. 181
Table 7.7: Rights of different roles associated with the objects before and after Replace model ......................................................... 182
Table 7.8: Owner and beneficiary rights over different objects before and after Replace model ......................................................... 182
Table 7.9: Output Summary of the Replace model ............................................................................................................................ 184
Table 7.10: Precedence of Replace model over other rights allocation models ................................................................................... 184
Table 7.11: Output summary of Share Use and Share Meta models ................................................................................................. 186
Table 7.12: Comparison of various characteristics of Share model .................................................................................................... 186
Table 7.13: Rights of different roles associated with the objects before and after Share model ......................................................... 187
Table 7.14: Owner and beneficiary rights over different objects before and after Share model ......................................................... 188
Table 7.15: Output Summary of the Share model ............................................................................................................................ 189
Table 7.16: Precedence of Share model applications over other rights allocation models ............................................................... 189
Table 7.17: Output summary of Merge Use and Merge Meta models ................................................................................................. 191
Table 7.18: Comparison of various characteristics of Merge model .............................................................. 191
Table 7.19: Rights of different roles associated with the objects before and after Merge model ......................... 192
Table 7.20: Owner and beneficiary rights over different objects before and after Merge model ........................... 193
Table 7.21: Output Summary of the Merge model........................................................................................... 194
Table 7.22: Precedence of Merge model applications over other rights allocation models .................................. 195
Table 7.23: All the Possible Options for Various Characteristics of Rights Allocation Framework ...................... 197
Table 7.1: Possible permutations for use-rights models ...................................................................................... 248
Table 7.3: Table depicting all possible cases for meta-rights models ................................................................. 250
List of Publications


### Terms used in formulae

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Admin</td>
<td>Administrator of a system</td>
</tr>
<tr>
<td>AC</td>
<td>Attestation Certificate</td>
</tr>
<tr>
<td>AU</td>
<td>Active Users</td>
</tr>
<tr>
<td>Ben</td>
<td>Beneficiary</td>
</tr>
<tr>
<td>D/C</td>
<td>Don’t Care condition</td>
</tr>
<tr>
<td>Dge</td>
<td>Delegatee</td>
</tr>
<tr>
<td>Dgr</td>
<td>Delegator</td>
</tr>
<tr>
<td>E</td>
<td>Entity</td>
</tr>
<tr>
<td>GP</td>
<td>General Public</td>
</tr>
<tr>
<td>JBen</td>
<td>Joint Beneficiary</td>
</tr>
<tr>
<td>JO</td>
<td>Joint Owner</td>
</tr>
<tr>
<td>LR</td>
<td>Local Role</td>
</tr>
<tr>
<td>MR</td>
<td>Meta-Right</td>
</tr>
<tr>
<td>Mrg</td>
<td>Merge</td>
</tr>
<tr>
<td>NS</td>
<td>Namespace</td>
</tr>
<tr>
<td>O</td>
<td>Object</td>
</tr>
<tr>
<td>OC</td>
<td>Object Class</td>
</tr>
<tr>
<td>Opr</td>
<td>Operation</td>
</tr>
<tr>
<td>PO</td>
<td>Primary Owner</td>
</tr>
<tr>
<td>R</td>
<td>Right</td>
</tr>
<tr>
<td>Rep</td>
<td>Replace</td>
</tr>
<tr>
<td>Rev</td>
<td>Revoke</td>
</tr>
<tr>
<td>S</td>
<td>Subject</td>
</tr>
<tr>
<td>SH</td>
<td>Stakeholder</td>
</tr>
<tr>
<td>Shr</td>
<td>Share</td>
</tr>
<tr>
<td>SO</td>
<td>Secondary Owner</td>
</tr>
<tr>
<td>VU</td>
<td>Virtual User</td>
</tr>
<tr>
<td>UR</td>
<td>Use-Right</td>
</tr>
</tbody>
</table>