

# University of Wollongong - Research Online

## Thesis Collection

Title: Detecting and resolving redundancies in EP3P policies

Author: Farzad Salim

Year: 2006

Repository DOI:

### Copyright Warning

You may print or download ONE copy of this document for the purpose of your own research or study. The University does not authorise you to copy, communicate or otherwise make available electronically to any other person any copyright material contained on this site.

You are reminded of the following: This work is copyright. Apart from any use permitted under the Copyright Act 1968, no part of this work may be reproduced by any process, nor may any other exclusive right be exercised, without the permission of the author. Copyright owners are entitled to take legal action against persons who infringe their copyright. A reproduction of material that is protected by copyright may be a copyright infringement. A court may impose penalties and award damages in relation to offences and infringements relating to copyright material.

Higher penalties may apply, and higher damages may be awarded, for offences and infringements involving the conversion of material into digital or electronic form.

**Unless otherwise indicated, the views expressed in this thesis are those of the author and do not necessarily represent the views of the University of Wollongong.**

Research Online is the open access repository for the University of Wollongong. For further information contact the UOW Library: [research-pubs@uow.edu.au](mailto:research-pubs@uow.edu.au)

2006

## Detecting and resolving redundancies in EP3P policies

Farzad Salim

*University of Wollongong*, [fsalim@uow.edu.au](mailto:fsalim@uow.edu.au)

Follow this and additional works at: <https://ro.uow.edu.au/theses>

### University of Wollongong

#### Copyright Warning

You may print or download ONE copy of this document for the purpose of your own research or study. The University does not authorise you to copy, communicate or otherwise make available electronically to any other person any copyright material contained on this site.

You are reminded of the following: This work is copyright. Apart from any use permitted under the Copyright Act 1968, no part of this work may be reproduced by any process, nor may any other exclusive right be exercised, without the permission of the author. Copyright owners are entitled to take legal action against persons who infringe their copyright. A reproduction of material that is protected by copyright may be a copyright infringement. A court may impose penalties and award damages in relation to offences and infringements relating to copyright material.

Higher penalties may apply, and higher damages may be awarded, for offences and infringements involving the conversion of material into digital or electronic form.

Unless otherwise indicated, the views expressed in this thesis are those of the author and do not necessarily represent the views of the University of Wollongong.

---

### Recommended Citation

Salim, Farzad, Detecting and resolving redundancies in EP3P policies, MCompSc thesis, School of Information Technology and Computer Science, University of Wollongong, 2006. <http://ro.uow.edu.au/theses/549>

## **NOTE**

This online version of the thesis may have different page formatting and pagination from the paper copy held in the University of Wollongong Library.

## **UNIVERSITY OF WOLLONGONG**

### **COPYRIGHT WARNING**

You may print or download ONE copy of this document for the purpose of your own research or study. The University does not authorise you to copy, communicate or otherwise make available electronically to any other person any copyright material contained on this site. You are reminded of the following:

Copyright owners are entitled to take legal action against persons who infringe their copyright. A reproduction of material that is protected by copyright may be a copyright infringement. A court may impose penalties and award damages in relation to offences and infringements relating to copyright material. Higher penalties may apply, and higher damages may be awarded, for offences and infringements involving the conversion of material into digital or electronic form.



# Detecting and Resolving Redundancies in EP3P Policies

A thesis submitted in fulfillment of the  
requirements for the award of the degree

**Master of Computer Science (Research)**

from

UNIVERSITY OF WOLLONGONG

by

**Farzad Salim**

School of IT and CS.  
September 2006

© Copyright 2006

by

Farzad Salim

All Rights Reserved

*Dedicated to*

*My Family*

# Declaration

This is to certify that the work reported in this thesis was done by the author, unless specified otherwise, and that no part of it has been submitted in a thesis to any other university or similar institution.

---

Farzad Salim  
September 7, 2006

# Abstract

---

Current regulatory requirements on data privacy make it increasingly important for enterprises to be able to verify and audit their compliance with their privacy policies. Traditionally, a privacy policy is written in a natural language. Such policies inherit the potential ambiguity, inconsistency and mis-interpretation of natural text. Hence, formal languages are emerging to allow a precise specification of enforceable privacy policies that can be verified.

The EP3P language is one such formal language. An EP3P privacy policy of an enterprise consists of many rules. Given the semantics of the language, there may exist some rules in the ruleset which can never be used, these rules are referred to as *redundant* rules.

Redundancies adversely affect privacy policies in several ways. Firstly, redundant rules reduce the efficiency of operations on privacy policies. Secondly, they may misdirect the policy auditor when determining the outcome of a policy. Therefore, in order to address these deficiencies it is important to identify and resolve redundancies.

This thesis introduces the concept of *minimal privacy policy* - a policy that is free of redundancy. The essential component for maintaining the minimality of privacy policies is to determine the effects of the rules on each other. Hence, redundancy detection and resolution frameworks are proposed. Pair-wise redundancy detection is the central concept in these frameworks and it suggests a pair-wise comparison of the rules in order to detect redundancies. In addition, the thesis introduces a policy management tool that assists policy auditors in performing several operations on an EP3P privacy policy while maintaining its minimality. Formal results comparing alternative notions of redundancy, and how this would affect the tool, are also presented.



# Acknowledgments

---

On completion of such a time-consuming journey, there are always many people to acknowledge. This thesis would have never been possible without them. It is a pleasant aspect that I have the opportunity to express my gratitude for all of them.

Firstly, I would like to express my sincere appreciation to both of my supervisors, Prof. Aditya Ghose and Prof. Rei Safavi-Naini for their guidance, encouragement and support through the course of this work. I would also like to thank Peter Harvey for his critical questions as well as supporting me at those times when my research encountered obstacles. Thanks also goes to Janos Tsakiris for proof reading my thesis.

I would like to acknowledge the friendship of Peter, Janos, Chee Fon, Victoria, Siamak, Sara, as well as that of Elinor, whose support during the thesis writing stage will not be forgotten. I'd especially like to thank my cousin Ehsan for bringing a smile to my face and providing motivation when times were tough.

I would like to express my deep and sincere gratitude to my father and mother who formed part of my vision and taught me to see the good in everything and be a constructive part of the whole. Their faith in me, advises, and encouragements provided a persistent inspiration for my journey in this life. I am grateful for my brother Farhad and my sisters Sara and Sohaila for always being there for me.

# Contents

---

<b>Abstract</b>	<b>v</b>
<b>Acknowledgments</b>	<b>vi</b>
<b>1 Introduction</b>	<b>1</b>
1.1 Motivation . . . . .	1
1.2 Contribution . . . . .	4
1.3 Thesis Structure . . . . .	5
<b>2 Background and Related Work</b>	<b>7</b>
2.1 Enterprises and Privacy Issues . . . . .	7
2.2 Privacy Policy Languages . . . . .	9
2.2.1 P3P . . . . .	10
2.2.2 APPEL . . . . .	12
2.2.3 EP3P . . . . .	14
2.2.4 EPAL . . . . .	19
2.2.5 XACML . . . . .	19
2.3 Limitations of Privacy Policy Languages . . . . .	19
2.3.1 P3P Language . . . . .	19
2.3.2 APPEL . . . . .	21
2.4 Policy Management Tools . . . . .	22
2.5 Privacy Policy Enforcement . . . . .	25
2.5.1 E-P3P Framework . . . . .	26
2.5.2 Tivoli Privacy Manager . . . . .	28
<b>3 EP3P Language &amp; Policy Management Operations</b>	<b>30</b>
3.1 EP3P Language . . . . .	30
3.1.1 EP3P Syntax . . . . .	30
3.1.2 EP3P Operational Semantics . . . . .	32
3.2 Desirable Attributes . . . . .	35
3.2.1 Consistency . . . . .	35

3.2.2	Safety . . . . .	37
3.2.3	Minimality . . . . .	37
3.3	Operations on Privacy Policies . . . . .	38
3.3.1	Policy Refinement . . . . .	38
3.3.2	Policy Composition . . . . .	39
3.3.3	Alignment of Privacy Promises with Privacy Practices . . . . .	40
3.3.4	Formalizing Privacy Policy in EP3P . . . . .	42
<b>4</b>	<b>Redundancy Detection Framework</b>	<b>45</b>
4.1	Illustrative Example . . . . .	45
4.2	Definitions of Redundancy . . . . .	46
4.3	Sources of Redundancy . . . . .	49
4.4	Redundancy Classification . . . . .	50
4.4.1	Includes . . . . .	52
4.4.2	Shadows . . . . .	53
4.4.3	Contradicts . . . . .	54
4.5	Rule Redundancy Model . . . . .	55
4.6	Pairwise Redundancy Detection . . . . .	56
4.6.1	Undetected Redundancies . . . . .	59
4.6.2	Redundancy Detection Algorithms . . . . .	59
<b>5</b>	<b>Redundancy Resolution Framework</b>	<b>65</b>
5.1	Pairwise Redundancy Resolution . . . . .	65
5.2	Ruleset Redundancy Resolution . . . . .	68
5.2.1	Dealing With Contradictory Suggestions . . . . .	68
5.2.2	Policy Compaction . . . . .	69
5.2.3	Policy Rectification . . . . .	71
5.2.4	Efficient Policy Rectification . . . . .	73
5.3	Maintaining an EP3P Privacy Policy . . . . .	76
5.3.1	Policy Update . . . . .	76
5.3.2	Policy Revision . . . . .	78
5.3.3	Changes in a Vocabulary . . . . .	79
<b>6</b>	<b>EP3P Policy Management Console</b>	<b>80</b>
6.1	System Design . . . . .	81
6.2	Graphical User Interface . . . . .	82
6.3	Formalizing A Privacy Policy . . . . .	83
6.3.1	Constructing EP3P Vocabulary . . . . .	83
6.3.2	Constructing EP3P Rules . . . . .	87

6.4	Redundancy Detection . . . . .	90
6.5	Redundancy Resolution . . . . .	91
<b>7</b>	<b>Conclusion</b>	<b>93</b>
<b>8</b>	<b>Future Work</b>	<b>96</b>
	<b>Bibliography</b>	<b>98</b>
<b>A</b>	<b><i>Medi-Care Hospital's EP3P Policy</i></b>	<b>103</b>
A.1	EP3P Vocabulary . . . . .	103
A.2	EP3P Rules . . . . .	107
<b>B</b>	<b><i>Medi-Care Hospital Application</i></b>	<b>109</b>
B.1	Class Diagrams & Sequence Diagrams . . . . .	109
B.2	Application's Source Code . . . . .	114
B.2.1	Editor.java . . . . .	114
B.2.2	TreeField.java . . . . .	130
B.2.3	TableField.java . . . . .	133
B.2.4	Rules.java . . . . .	137
B.2.5	Vocabulary.java . . . . .	140
B.2.6	Redundancies.java . . . . .	142
B.2.7	Duplicates.java . . . . .	149

# List of Figures

---

2.1	P3P Policy . . . . .	12
2.2	APPLE Preferences . . . . .	13
2.3	Data User Hierarchy . . . . .	15
2.4	Data Type Hierarchy . . . . .	15
2.5	Purpose Hierarchy . . . . .	16
2.6	EP3P Vocabulary . . . . .	17
2.7	EP3P Rules . . . . .	18
2.8	EP3P Enforcement Model . . . . .	27
2.9	Tivoli: Privacy Enforcement . . . . .	28
4.1	Simplified Vocabulary . . . . .	45
4.2	Interaction of rules with respect to user, data and purpose hierarchies . . . . .	51
4.3	Covering Relation . . . . .	52
4.4	Redundancy Situation: Including . . . . .	53
4.5	Redundancy Situation: Shadowing . . . . .	54
4.6	Redundancy Situation: Contradicts . . . . .	55
4.7	Redundancy Relation . . . . .	56
6.1	Policy Management Console Block Diagram . . . . .	82
6.2	Data Categories . . . . .	84
6.3	User Categories . . . . .	84
6.4	Purpose Categories . . . . .	84
6.5	Specifying User, Data and Purpose Hierarchies . . . . .	85
6.6	Specifying Action, Condition and Obligations . . . . .	87
6.7	Specifying Authorization Rules . . . . .	89
6.8	Redundancies . . . . .	91
6.9	Redundancies . . . . .	92