2006

Detecting and resolving redundancies in EP3P policies

Farzad Salim
University of Wollongong, fsalim@uow.edu.au

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

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

List of Figures