

University of Tasmania Open Access Repository

Cover sheet

Title

Professional Access Control

Author

de la Motte, L

Bibliographic citation

de la Motte, L (2004). Professional Access Control. University Of Tasmania. Thesis.
<https://doi.org/10.25959/23213255.v1>

Is published in:

Copyright information

This version of work is made accessible in the repository with the permission of the copyright holder/s under the following,

Licence.

If you believe that this work infringes copyright, please email details to: oa.repository@utas.edu.au

Downloaded from University of Tasmania Open Access Repository

Please do not remove this coversheet as it contains citation and copyright information.

University of Tasmania Open Access Repository

Library and Cultural Collections

University of Tasmania

Private Bag 3

Hobart, TAS 7005 Australia

E oa.repository@utas.edu.au

CRICOS Provider Code 00586B | ABN 30 764 374 782

utas.edu.au

Professional Access Control

by

Leigh Howard de la Motte, B.Comp.

A dissertation submitted to the
School of Computing
in partial fulfilment of the requirements for the degree of

Bachelor of Computing with Honours

University of Tasmania

November 2004

Declaration

I, Leigh de la Motte, declare that this thesis contains no material which has been accepted for the award of any other degree or diploma in any tertiary institution. To my knowledge and belief, this thesis contains no material previously published or written by another person except where due reference is made in the text of the thesis.

Leigh de la Motte

Abstract

Professional Access Control (PAC) is a self-administrating access control model for professional users which employs a peer review process and oversight by system administrators. It is characterised by the existence of ethical controls on the relationships between the users (those accessing data or granting access privileges to others) and data owners. Investigations revealed that the issue of availability was crucial to users in the hospital domain studied, and that to minimise the administrative burden on system administrators, the users needed to take some of the load. These factors led to the development of the new Trusted Access Control (TAC) model which gives users control. TAC is a fundamental access control model, complementary to the well-known Mandatory Access Control (MAC) and Discretionary Access Control (DAC) models. PAC uses TAC at its core and also incorporates Role Based Access Control (RBAC) and Provision Based Access Control (PBAC). This gives it the flexibility and user-friendliness necessary in the hospital environment, while still providing a high degree of data confidentiality and integrity protection. The required PAC functionality has been built into an Oracle package which can be used by new and existing applications, making it a viable access control solution for complex environments such as hospitals. When enabled workflow applications use the Oracle package, access control is automatically effected behind-the-scene, providing both usability benefits and reduced administrative burden.

Acknowledgements

Special thanks go to my Supervisor, Jacky Hartnett, for her patience and her ability to keep me on track. The encouragement she gave made the whole process much more pleasant. Her advice on security concepts and insightful comments regarding my work, were extremely important.

Peter Vamplew and Jacky Hartnett provided good support and advice in their roles as Honours Coordinators.

I would also like to thank all the health practitioners and administrators that have contributed ideas. Especially, thanks to Chris Showell and Justin Thurley, from the Department of Health and Human Services, for their time and input into this project. Their advice and comments greatly assisted the development of a practical solution.

Christian McGee and Greg Frith were very helpful with assisting me to set up Oracle. Andrew Spilling and Rick Smith provided great tech support during the year. My thanks also go to Claire Tomlim and Heather de la Motte for proof reading this document.

Finally, thank you to all my honours colleagues, who have always made themselves available to assist when asked. Particular thanks go to Tim Everts, Barry Pearn and Chris MacLeavy for their help with managing the idiosyncrasies of Microsoft Word, among other things.

Table of Contents

Chapter 1

Introduction	1
---------------------------	----------

Chapter 2

Background.....	5
2.1 Patient Medical Records	5
2.1.1 EHRs, Data ownership, Consent and Duty of Care.....	5
2.1.2 Increasing Threats against Medical Records.....	6
2.2 Hospital Environment	7
2.2.1 Patient Movement.....	8
2.2.2 Staff Movement	8
2.2.3 Openness to the Public	8
2.3 The Professional Environment and Ethics	8
2.3.1 System Admin vs Professional Decisions.....	9
2.4 Implementation Requirements	10
2.5 Hospital Environment Pros and Cons	12
2.6 Discussion	13
2.6.1 Who Makes Authorisation Decisions?.....	13
2.6.2 Business Rules and Policies	14
2.6.3 Summary	15

Chapter 3

Related Work.....	16
3.1 Basic Access Control Terminology	16
3.2 Mandatory and Discretionary Access Control:	17
3.3 Role Based Access Control:.....	20
3.4 Team-based Access Control:.....	22
3.4.1 TMAC Versions	22
3.4.2 TMAC Deficiencies	23
3.5 Task-Based Access Control:	25

3.6	Organisation-Based Access Control:	25
3.7	Provisional Authorisation Models:	26
3.8	Auditing:	27
3.9	Clark-Wilson:	28
3.10	Middleware:	28
3.11	Review of Existing Models	29

Chapter 4

Method	31
4.1 Workflow Analysis	32
4.2 Model Analysis	32
4.3 Team Definition	32
4.4 Model Development	33
4.5 Model Implementation	34
4.6 Functional Testing	36
4.6.1 Testing Procedure	38
4.6.2 Testing Sequence	38
4.7 Scenario Verification	39

Chapter 5

Results and Discussion	40
5.1 Hospital Scenarios	40
5.2 Models	42
5.2.1 The Trusted Access Control (TAC) Model	42
5.2.2 The Professional Access Control (PAC) Model	46
5.3 Oracle PAC Toolkit	57
5.4 Simulation Test Results	59
5.5 Validation Results	61

Chapter 6

Conclusion	65
-------------------------	-----------

Chapter 7

Further Work	69
--------------------	----

Chapter 8

References	71
------------------	----

Appendices

Appendix A – Simulation Test Results	i
Appendix B – Simulation Test Notes	xvii
Appendix C – Database Scripts and Test Data.....	xxiv

List of Figures

Figure 1: Player Categories.....	16
Figure 2: General Access Control Principles.....	17
Figure 3: Mandatory Access Control.....	18
Figure 4: Discretionary Access Control.....	19
Figure 5: Role-Based Access Control.....	20
Figure 6: Team-Based Access Control.....	22
Figure 7: Team Concept Differences.....	24
Figure 8: Provisional Access Control.....	26
Figure 9: Method Flow Diagram.....	31
Figure 10: Foundational Access Control Models.....	43
Figure 11: Trusted Access Control.....	44
Figure 12: Staff Roles and Units.....	48
Figure 13: Team Staff Categories.....	49
Figure 14: Professional Access Control.....	50
Figure 15: PAC Access Method #1.....	53
Figure 16: PAC Access Method #2.....	54
Figure 17: PAC Access Method #3.....	55
Figure 18: PAC Access Method #4.....	55
Figure 19: Applications using the Oracle PAC Toolkit.....	58

List of Tables

Table 1: Hospital Scenarios.....	42
Table 2: Example of the Current Hospital State Table.....	59
Table 3: Example of the Changes Table.....	60
Table 4: Simulation Test Results.....	62
Table 5: Scenario Functionality Checking.....	64