Secure Information Flow for Inter-organisational Collaborative Environments

Shane Bracher
BIT, MIT (Hons) (Bond)

A dissertation submitted in fulfilment of the requirements of the degree of Doctor of Philosophy for the School of Information Technology, Bond University.

April 2009
Statement of Originality

The work presented in this thesis is, to the best of my knowledge and belief, original, except where acknowledged in the text. I hereby declare that I have not submitted this material either in whole or in part, for a degree at this or any other university.

Shane Bracher
Date:
Abstract

Collaborative environments allow users to share and access data across networks spanning multiple administrative domains and beyond organisational boundaries. This poses several security concerns such as data confidentiality, data privacy and threats to improper data usage. Traditional access control mechanisms focus on centralised systems and implicitly assume that all resources reside in the one domain. This serves as a critical limitation for inter-organisational collaborative environments, which are characteristically decentralised, distributed and heterogeneous.

A consequence of the lack of suitable access control mechanisms for inter-organisational collaborative environments is that data owners relinquish all control over data they release. In these environments, we can reasonably consider more complex cases where documents may have multiple contributors, all with differing access control requirements. Facilitating such cases, as well as maintaining control over the document’s content, its structure and its flow path as it circulates through multiple administrative domains, is a non-trival issue.

This thesis proposes an architecture model for specifying and enforcing access control restrictions on sensitive data that follows a pre-defined inter-organisational workflow. Our approach is to embed access control enforcement within the workflow object (e.g. the circulating document containing sensitive data) as opposed to relying on each administrative domain to enforce the access control policies. The architecture model achieves this using cryptographic access control – a concept that relies on cryptography to enforce access control policies.

The specifications for the architecture model, as well as the specifications for an workflow object model, are discussed in this thesis. The workflow object model supports finer-granularity access control (on the content level) and describes how the workflow object encapsulates sensitive data, together with metadata defining the access rights. A prototype implementation of the models was constructed for experimentation purposes. Using this prototype, case studies were conducted to demonstrate the feasibility of the proposed models and to identify potential applications.
Acknowledgements

This thesis would not have been possible without the support of many people and organisations to whom I express my gratitude. In particular, I would like to thank:

Dr Padmanabhan (Paddy) Krishnan, for his supervision, advice, encouragement, enthusiasm and commitment throughout my PhD candidature. Whenever I needed assistance, you were always available to answer my questions, share ideas and offer valuable feedback.

Dr Jorge Cuellar, for his supervision during my internship at Siemens AG (Corporate Technology) and ideas for my research.

Dr Zheng da Wu, for his guidance during the early stages of my PhD candidature and also during my honours research.

The School of Information Technology, Bond University, for providing the resources needed to complete my PhD. I also extend my gratitude to all staff and students in the School, past and present, who have helped me and made my time at Bond all the more enjoyable.

The Australian Government, for supporting me with an Australian Postgraduate Award.

Fellow PhD candidates and officemates James Larkin and Percy Pari-Salas, for the discussions, humour, assistance and for creating a great office atmosphere.

My colleagues and officemates at Siemens: Dr Joerg Abendroth, Dong Huang, Dr Anja Jerichow, Assadarat Khurat, Dr Monika Maidl, Hariharan Rajasekaran, Dr David von Oheimb and all staff and students who helped make my stay such a pleasant experience.

Finally, my family, for their continuous support and encouragement. Thank you.
## Contents

1 Introduction 1

1.1 Objectives .................................................. 4
1.2 Deliverables ............................................... 5
1.3 Thesis Structure ......................................... 6

2 Literature Review 7

2.1 Workflow Management ................................. 7
  2.1.1 Workflow Concepts ................................. 7
  2.1.2 Workflow Frameworks .............................. 9
  2.1.3 Workflow Patterns ................................. 12
  2.1.4 Workflow Implementation Models ............... 15

2.2 Security Policies and Access Control ................. 18
  2.2.1 Security Concepts .................................... 18
  2.2.2 Security Policies and Models .................... 25
  2.2.3 Traditional Access Control Models ............... 33
  2.2.4 Implementing Access Control .................... 37
  2.2.5 Emerging Access Control Technologies .......... 38

2.3 Access Control for Inter-organisational Workflows 45

2.4 Cryptographic Access Control .......................... 46

2.5 Summary .................................................. 48
## 3 Architecture Model

3.1 Overview .................................................. 49
3.2 Example Workflow ....................................... 52
3.3 User-based Model ......................................... 53
3.4 Role-based Model .......................................... 54
3.5 Workflow Instantiation .................................... 55
3.6 Key Exchange ............................................... 56
  3.6.1 User-defined Shared Keys ............................ 58
3.7 Access Types ............................................... 59
  3.7.1 Read Only Access ..................................... 60
  3.7.2 Read Write Access ................................... 60
  3.7.3 Append Access ........................................ 61
3.8 Workflow Object History ................................ 63
3.9 Multiple Domains ......................................... 65
3.10 Multiple Permissions ...................................... 68
3.11 Identity Provider as Verifier ........................... 69
3.12 Summary .................................................. 70

## 4 Workflow Object Model

4.1 Components ................................................ 71
4.2 Specifications .............................................. 73
  4.2.1 Object Data Component ............................... 74
  4.2.2 Object Metadata Component .......................... 74
  4.2.3 Schema Component ................................... 75
  4.2.4 Policies Component ................................... 76
  4.2.5 Template Component .................................. 77
4.3 Summary .................................................. 77

## 5 Prototype Implementation

5.1 Overview .................................................. 78
5.2 Workflow Engine ........................................... 80
5.3 Identity Provider .......................................... 82
  5.3.1 Identity Management .................................. 83
  5.3.2 Key Management ...................................... 84
5.4 Document Processing Environment ....................... 86
5.5 Summary .................................................. 89

6 Case Studies .................................................. 90
  6.1 Case Study 1 – Loan Application ......................... 90
    6.1.1 Process ............................................... 91
    6.1.2 Document Design .................................... 93
    6.1.3 Users and Roles .................................... 96
    6.1.4 Implementation .................................... 97
    6.1.5 Discussion .......................................... 101
  6.2 Case Study 2 – Electronic Health Records .............. 103
    6.2.1 Process ............................................... 103
    6.2.2 Document Design .................................... 106
    6.2.3 Users and Roles .................................... 107
    6.2.4 Implementation .................................... 108
    6.2.5 Discussion .......................................... 112
  6.3 Case Study 3 – Wildlife Report .................... 114
    6.3.1 Policies .............................................. 115
    6.3.2 Document Design .................................... 115
    6.3.3 Implementation .................................... 116
    6.3.4 Discussion .......................................... 116
  6.4 Lessons Learned ......................................... 117
  6.5 Summary .................................................. 119

7 Conclusion .................................................. 121
  7.1 Contributions ........................................... 122
List of Figures

2.1 Workflow reference model. ................................................. 10
2.2 Workflow perspectives. .................................................. 11
2.3 Web services base model. ................................................ 17
2.4 The basic model for conventional encryption. ...................... 19
2.5 The basic model for public-key encryption. ......................... 20
2.6 Chinese Wall data hierarchy. ............................................ 26
2.7 Bell-LaPadula model example. ........................................ 28
2.8 ORCON example. ............................................................ 29
2.9 ORCON with UCON example. ........................................... 30
2.10 A typical DRM system. ................................................... 32
2.11 ACL and capability list examples. ..................................... 35
2.12 The Role-Based Access Control model (Core RBAC). ............. 37
2.13 The SAML producer-consumer model. ............................. 40
2.14 The XACML architecture. ............................................... 42
2.15 The Web Services Security framework. ............................. 43
3.1 Simplified view of the architecture model. ......................... 51
3.2 Example workflow used for subsequent explanations of the architecture model. . 52
3.3 Request/response procedure for obtaining shared key. ............ 58
3.4 Example workflow modified to include multiple domains. ........ 66
3.5 Architecture extension to support verification by identity providers. .... 69
4.1 The workflow object model components. ........................... 72
5.1 Overview of the prototype implementation setup. .......................... 79
5.2 Workflow simulation setup for prototype. ................................. 81
5.3 Parallel transitions. ......................................................... 81
5.4 Intermediary transitions. ..................................................... 82
5.5 Identity management system setup. ......................................... 84
5.6 Key management setup for prototype. ..................................... 85
5.7 Document processing environment setup. .................................. 87

6.1 Loan application workflow. .................................................. 91
6.2 Top-level view of document data component. ............................. 94
6.3 Document data component section for processing. ....................... 95
6.4 Top-level view of document metadata component. ....................... 95
6.5 Protected data items section in document metadata component. .... 95
6.6 Screenshot of loan application form. ....................................... 99
6.7 Screenshot of protected data items on form. ............................... 100
6.8 Medical record workflow. .................................................... 104
6.9 Workflow history section in document metadata component. ......... 106
6.10 Top-level view of medical record schema. ............................... 106
6.11 Screenshots of verifier interface. .......................................... 110
6.12 Remodelled medical record workflow. .................................... 111
6.13 Modified design for protected data item records. ....................... 116